Université Paris II- Panthéon-Assas

école doctorale de Droit privé

Thèse de doctorat en droit
soutenue le 7 décembre 2018

Thèse de Doctorat / Décembre 2018

La protection des libertés individuelles sur le réseau internet

UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

Auteur : Géraldine CRIQUI-BARTHALAIS

Sous la direction de Monsieur **Jérôme HUET**
Professeur émérite à l'Université Panthéon-Assas (Paris II)

Membres du jury :
Madame **Anne DEBET**
Professeure à l'Université de Paris-Descartes (Paris V), rapporteur
Madame **Célia ZOLYNSKI**
Professeure à l'Université Versailles Saint-Quentin
Monsieur **Emmanuel DREYER**
Professeur à l'Université Panthéon-Sorbonne (Paris 1), rapporteur
Monsieur **Cédric MANARA**
Docteur en droit, juriste d'entreprise

Avertissement

La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur.

Mes remerciements vont à :

M. le professeur Jérôme Huet pour sa direction bienveillante et son enseignement. Je le remercie également d'avoir inscrit ce travail de thèse dans le cadre de l'activité du CEJEM, un laboratoire dynamique et à notre service. Echanger avec d'autres doctorants et professionnels, et se former à la rédaction dès les premières années de thèse, ont fait beaucoup pour ces recherches.

Mes parents, Marie-Reine et Etienne, pour tout. Je remercie mon père plus particulièrement pour ses encouragements et ses relectures attentives et ma mère pour sa présence et le goût qu'elle m'a transmis des nouvelles technologies.

Ma sœur, Juliette, pour son soutien et pour ses conseils judicieux de vidéos et d'applications. Mon frère, Olivier, pour son affection et son humour.

Mes beaux-parents, Donatella et Bruno, pour leur accueil chaleureux dans leur famille et leur disponibilité.

Mon amie d'enfance, Clothilde, qui a toujours les mots justes.

Claire S.C., Anabel R.S., Marie B.C., pour les bons moments partagés qui en laissent présager beaucoup d'autres alors que toutes, nous avons maintenant fini notre thèse !

Caroline L.G., pour ses conseils et son dynamisme communicatif, depuis les TD à Melun jusqu'à ces derniers mois de thèse.

Octavie L., Asma A., Hussein K., Jérôme C., pour le quotidien partagé au laboratoire de sociologie juridique, à la fois studieux et détendu.

Nathalie Ceriani qui, du secrétariat du CEJEM à celui du laboratoire de sociologie juridique, m'a toujours témoigné de la sympathie.

Mme la professeure Dominique Fenouillet, directrice du laboratoire de sociologie juridique, pour m'avoir permis de terminer ma thèse dans des conditions idéales.

Mon mari, Stéphane. Ce travail n'aurait pas pu aboutir sans sa présence, sa gentillesse et sa générosité. Je le remercie d'avoir toujours envisagé cette thèse comme un projet commun. Son calme, son énergie, et sa joie de vivre nous ont permis d'en accomplir beaucoup d'autres.

A Stéphane, mon mari

et à Gabriel, notre fils

Résumé :
Cette étude envisage le réseau internet comme un nouvel espace invitant à réinterpréter les libertés de la personne physique. Au titre de celles-ci, sont protégées la liberté individuelle, entendue comme le fait de ne pouvoir être arbitrairement détenu et la liberté d'aller et venir. Il doit en aller de même sur le réseau. Etablissant une analogie avec ces libertés, la première partie de la thèse consacre deux libertés : la liberté d'accès au réseau et la liberté de naviguer sur le web. La première implique de définir le contenu d'un service public de l'accès. De plus, il faut affirmer que la coupure d'accès au réseau doit être envisagée comme une mesure privative de liberté ; elle ne peut donc être décidée que par le juge judiciaire. L'affirmation de la liberté de naviguer sur le web conduit à envisager le régime du blocage des sites, une mesure qui ne peut intervenir que dans le cadre d'une police administrative spéciale. Dans la seconde partie il apparaît que ces deux libertés n'ont toutefois de sens que si l'individu a accès au réseau anonymement et n'est pas surveillé arbitrairement quand il navigue sur le web. Cette étude cherche ainsi à préciser le régime devant encadrer le mécanisme d'adressage du réseau. Sont définies les conditions du contrôle de l'identité de l'internaute à partir de son adresse IP. Enfin, il est soutenu qu'un principe général d'effacement des données révélant les sites visités doit être affirmé, principe qui s'applique aux différents acteurs du réseau, notamment les moteurs de recherche. L'interception de ces données ne peut procéder que d'un pouvoir sécuritaire ou hiérarchique sur l'internaute.

Descripteurs :
Libertés publiques – Internet- Numérique- Communications électroniques- Accès au réseau- Anonymat sur le réseau- Adresse IP- Données personnelles- Surveillance- Informatique et libertés.

Title and Abstract: The protection of Individuals rights on the internet
This study considers the internet as a new territory where rights guaranteed to each individual in physical space can be promoted; not only free speech and privacy, but also the *Habeas Corpus* prerogative writ, which protects against unlawful imprisonment, and the right to freedom of movement. Thus, processing by analogy, the dissertation intends to promote two specific digital rights: the freedom to connect to the internet and the freedom to surf on the web. The freedom to connect should be part of a public service which promotes this access through public policies. Moreover, barring someone from using the internet can only be decided by a judge. The freedom to surf should protect the web users against unreasonable restrictions. Thus, measures blocking illegal websites should not come through self-regulation but through a legal framework which defines how administrative authorities are entitled to decide such restrictions. The protection of these two rights entails further obligations. Individuals must access the internet anonymously and they must be aware of how the government monitors their actions on the web. This study tries to outline the content of measures aiming to frame network addressing mechanisms. Identity checks based on the IP address should be subject to a strict legal regime. The study concludes that individuals have to be protected from surveillance when data reveal their choices among websites while they are connected. Internet access providers, but also search engines and browsers, must delete this data. Only special measures taken by a public entity or someone entitled to control the web users may lead to this kind of data retention.

Keywords:
Individuals rights-Digital rights- Internet- Electronic communications- Freedom to connect-Anonymity on the Internet-IP address-Surveillance-Data protection

Principales abréviations et sigles

aff.	Affaire
AJDA	Actualité juridique de droit administratif
al.	Alinéa
anc.	Ancien
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARCEP	Autorité de Régulation des Communications Electroniques et des Postes
art.	Article
ARJEL	Autorité de Régulation des Jeux En Ligne
Bull.	Bulletin des arrêts de la Cour de cassation (chambres civiles)
Bull. crim.	Bulletin des arrêts de la Cour de cassation (chambre criminelle)
BOCC	Bulletin Officiel de la Concurrence, de la Consommation et de la répression des fraudes
CA	Cour d'Appel
Cass. civ.	Cour de cassation, chambre civile
Cass. com.	Cour de cassation, chambre commerciale
Cass. crim.	Cour de cassation, chambre criminelle
CE	Conseil d'État
CEDH	Cour Européenne des Droits de l'Homme
Conv.EDH	Convention Européenne des Droits de l'Homme
CEJEM	Centre d'Etudes Juridiques et Economiques du Multimédia
CGLPL	Contrôleur Générale des Lieux de Privation de Liberté
CGU	Conditions Générales d'Utilisation
CJCE	Cour de Justice des Communautés Européennes
CJUE	Cour de Justice de l'Union Européenne
CNCTR	Commission Nationale de Contrôle des Techniques de Renseignement
CNIL	Commission Nationale de l'Informatique et des Libertés
CNNum	Conseil National du Numérique
Coll.	Collection
comm.	Commentaires
contra	En sens contraire
CCE	Communication Commerce Electronique

CCC	Contrats Concurrence Consommation
CP	Code pénal
CPC	Code de procédure civile
CPI	Code de la propriété intellectuelle
CPP	Code de procédure pénale
CPCE	Code des postes et des communications électroniques
CSI	Code de la sécurité intérieure
D.	Recueil Dalloz
DP	Dalloz Périodique
Dalloz IP/IT	Dalloz droit de la propriété intellectuelle et du numérique
DADVSI	Droit d'Auteur et Droit Voisins dans la Société de l'Information
DC	Décision de conformité
DDHC	Déclaration des Droits de l'Homme et du Citoyen
dir.	Direction
Dir.	Directive
DNS	Domain Name Système
Dr. pén.	Revue de droit pénal
éd.	Edition
FAI	Fournisseurs d'Accès à Internet
FCC	Federal Communications commission
FTC	Federal Trade commission
Gaz. Pal.	Gazette du Palais
HADOPI	Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet
ICANN	Internet Corporation for Assigned Names and Numbers
ibid.	*ibidem,* au même endroit
infra	ci-dessous
IP	Internet Protocol
JCP G	Jurisclasseur périodique, édition générale
JCP adm.	Jurisclasseur périodique, édition Administrations et Collectivités territoriales
JORF	Journal Officiel de la République Française
JOUE	Journal Officiel de l'Union européenne
JurisData	Juris-Data (Base de données du site internet Lexis-Nexis)
JurisPTT	JurisPTT, la revue du droit des PTT
LCEN	Loi pour la Confiance en l'Économie Numérique
LOPPSI	Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure

LPA	Les Petites Affiches
obs.	observations
OCLCTIC	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la communication
op. cit.	*opere citato* – dans l'ouvrage cité
ord.	ordonnance
p.	page
P2P	Peer-to-Peer
P.U.F.	Presse Universitaire de France
QPC	Question Prioritaire de Constitutionnalité
RD publ.	Revue de droit public
réf.	Référé
REM	Revue Européenne des Médias
Rép. Dalloz	Répertoire Dalloz
RLDI	Revue Lamy Droit de l'Immatériel
RTD civ.	Revue trimestrielle de droit civil
RTD com.	Revue trimestrielle de droit commercial
RSC	Revue de sciences criminelles
somm.	Sommaire
suiv.	Suivants
supra	ci-dessus
TGI	Tribunal de Grande Instance
URL	Uniform Resource Locator
V.	Voir

Sommaire

Quand il y a plus de vingt ans,
nous jouions avec fièvre au premier ping-pong électronique,
pensions-nous une seconde que nous serions ridicules
aux yeux de la nouvelle génération,
pitoyables pour la génération suivante et misérables pour celle d'après ?
Mais la fierté d'avoir été les premiers Homo Electronicus,
ne nous sera jamais enlevée.
Pionniers nous fûmes, et pionniers nous resterons.
Nous avons su où se dessinait l'Avenir.
Une humanité où tous les hommes regardent enfin
dans la même direction,
celle de leur écran d'ordinateur.

Lewis Trondheim, *Ordinateur mon ami,* Dargaud, Poisson Pilote, 2008

INTRODUCTION

1. **Notre « liberté chérie »**. « Liberté Chérie » est le titre choisi par le chanteur français Calogero pour son septième album[1] qu'il a voulu comme une réponse au climat de terreur, ressenti par tous, après les attentats ayant frappés Charlie Hebdo, le Bataclan et Paris en 2015, et Nice l'année suivante. Le chanteur, très marqué émotionnellement, a décidé d'enregistrer ce nouvel album à Londres, dans les studios d'Abbey Road, pour retrouver de l'énergie et de la joie. Le public a pu découvrir à l'été 2017 ces titres entrainants et lumineux au moment même où la capitale britannique était elle aussi touchée par une série d'attaques.

Cet album traduit avec justesse les préoccupations d'une génération qui ayant vécu son adolescence dans les années 80 ne peut concevoir cette violence qui nie la liberté de celles à venir. De manière fine, les chansons évoquent ces émotions mêlées de soif de liberté et de nostalgie. La chanson « Fondamental », dont les paroles sont signées Paul Ecole, est touchante, avec ces mots : « *Toutes ces pierres semées dans le passé, qui nous poussent et qui nous font pousser, cachées là au fond du mental, ce sont les choses fondamentales. On a tous, toutes ces choses fondamentales* ».

Pourtant le difficile est là : sentir concrètement, brutalement, la différence de choses fondamentales entre de jeunes terroristes, et nous, du même âge ; jeunes adultes qui avons pourtant été marqués par la même révolution, celle d'internet.

2. **La « révolution numérique »**. Dans son ouvrage « *Le Monde d'hier, souvenir d'un Européen* », paru en 1944, l'auteur autrichien Stefan Zweig témoigne de son admiration pour le poète belge Verhaeren et le décrit ainsi : « *Il s'était pris à aimer le monde moderne et voulait le conquérir à la poésie. Tandis que pour les autres la machine était le mal, les villes le hideux, le présent l'antipoétique, chaque nouvelle découverte, chaque réalisation technique suscitait son enthousiasme, et il s'enthousiasmait de son propre enthousiasme : il s'enthousiasmait de propos délibéré, pour se sentir plus fort de cette passion* »[2].

[1] CALOGERO, *Liberté chérie*, 2017, Polydor (France).
[2] ZWEIG Stefan, *Le Monde d'hier souvenirs d'un européen*, Bermann-Fisher Verkag AB Stockholm, 1944 (Belfond, Le Livre de Poche, Editions 1er coffret, novembre 2011, p.148).

Cet enthousiasme traduit bien celui de la génération des « Millenials »[3] : ils sont nés avec l'informatique et ont assisté à son développement fulgurant jusqu'au jour où le modem internet est arrivé dans leurs foyers, trônant au dessus de l'ordinateur. Ils peuvent encore entendre le bruit caractéristique de la connexion qui se faisait via la ligne téléphonique et ressentir cette excitation d'alors : le monde était là et à eux. C'était l'époque où l'on ne cherchait rien sur le web mais l'on surfait dessus, où l'on retrouvait les fameux cousins émigrés en Amérique via des courriels improbables, où l'on parlait à des inconnus sur Caramail, où enfin après avoir été privé de ce plaisir de faire des compilations de musiques sur cassette audio, on mettait à disposition son C.D de Patrick Bruel et l'on découvrait Elvis et Barbara via des fichiers MP3.

Toutefois, cette explosion du réseau et de ses possibilités à la fin des années 1990 coïncide également avec un autre évènement marquant : les attentats du 11 septembre 2001, qui ont bouleversé le monde et opéré un tournant dans l'approche de ces nouvelles technologies, et de nos libertés.

3. **La société du risque et de la sécurisation.** En effet, le monde de l'après 11 septembre est marqué par une évolution du principe de sûreté. A l'origine, celle-ci s'envisage comme une liberté. Comme l'énonce de manière remarquable Montesquieu dans *L'esprit des lois* : « *La liberté politique, dans un citoyen, est cette tranquillité d'esprit qui provient de l'opinion que chacun a de sa sûreté ; et pour qu'on ait cette liberté, il faut que le gouvernement soit tel, qu'un citoyen n'ait pas à craindre un autre citoyen* »[4].

Malheureusement cette tranquillité d'esprit n'est plus là au tournant du XXIème siècle et les frontières du rôle de l'État sont brouillées. Ainsi le professeur de droit public, Xavier Bioy expose dans son manuel de libertés fondamentales, que le mot sûreté est en proie à une forte ambigüité sémantique alors qu'il glisse du « *droit individuel* » vers le « *principe de protection de la société* » ; il souligne que « *Le droit utilise le terme de sûreté dès qu'il est question de sécuriser quelqu'un ou quelque chose, jusqu'aux sûretés réelles du droit des biens* »[5]. La sûreté de la révolution opposée à l'arbitraire du pouvoir dérive vers un principe de sécurisation qui semble devoir répondre aux incertitudes du monde et de la vie quotidienne.

[3] Aussi appelée la génération « Y », ou encore visant les « Digital natives ». Ces termes désignent généralement l'ensemble des personnes nées entre 1980 et l'an 2000.

[4] MONTESQUIEU, *De l'esprit des lois,* Paris : Garnier-Flammarion, 1979, tome I, p. 294.

[5] BIOY Xavier, *Droits fondamentaux et libertés publiques*, Paris : Montchrestien, Lextenso éditions, 2013 (LMD édition, Collection cours, *dir.* B. Beignier), n °1185, p.446.

La problématique est que ce développement de sociétés dites « *assurantielles* »[6] est nourri par celui des nouvelles possibilités technologiques qui permettent d'envisager un contrôle de ces risques. Ou inversement, alors qu'il est difficile de dissocier la cause de l'effet, le développement de la technique nourrit ce fantasme de la prédiction des comportements et d'un monde dès lors plus sûr.

4. **L'évolution de la surveillance.** Dans leur article traitant de l'intensification de la surveillance, la professeure Kirstie Ball et le sociologue Franck Webster utilisent l'expression de « surveillance compulsive »[7]. Celle-ci traduit bien le caractère de réponse immédiate que revêt la surveillance pour faire taire l'angoisse du monde dit de « *l'après 11 septembre* ». Le choix du terme « compulsion » renvoie également au caractère automatique de ces nouveaux procédés techniques qui peuvent être mis en œuvre à grande échelle : ils font croire à une efficacité nouvelle. Comme ces chercheurs l'expliquent, le ressort de la surveillance au début des années 2000 est ainsi : « *If only everything can be observed, then goes the reasoning everything may be controlled* »[8].

La professeure à l'Institut d'Études politiques de Paris, Ayse Cehan fait le même constat : « *C'est comme si la technologie et la biopolitique devenaient l'ultime moyen de sécuriser l'(in)sécurité et de gouverner le futur dans un monde de risques, d'incertitudes et de peurs* »[9]. Le chercheur Frédéric Ocqueteau affirme pour sa part que : « *La distinction entre le risque et la menace s'estompe au profit d'une culture émergente de la vulnérabilité* » ; il fait apparaître le caractère actuel de la surveillance qui repose sur une « *technologisation des contrôles* »[10].

A l'échelle d'internet, cette évolution fait naître le spectre d'un contrôle de l'individu via la structure du réseau et la collecte des données produites par chaque communication. L'image reprise par beaucoup est évidemment celle du Panoptique de Foucault qui a pour effet d'assurer le fonctionnement automatique du pouvoir. En effet Michel Foucault prend ici l'image du *Panopticon* de Bentham qui est une figure architecturale. Une tour est encerclée par un anneau divisé en cellules, percées de part

[6] Nous empruntons cette expression à François Ewald. V. : EWALD François, « Le Triomphe de la notion de risque » extraits de *L'état-providence* (Paris : Grasset, 1986) *in Problèmes politiques et sociaux,* La Documentation Française, octobre 2007, n°941, p. 17.

[7] BALL Kirstie, WEBSTER Franck, "The intensification of surveillance"*, in "The intensification of surveillance, Crime, terrorism and warfare in the information age",* Ball Kirstie and Frank Webster (*dir.)* London : Pluto Press, 2003,p.5

[8] *Ibid.* p. 4.

[9] CEHAN Ayse, « Sécurité, frontières et surveillance aux États-Unis après le 11 septembre 2001 », *in* « Surveillance politique, regards croisés », *Cultures et Conflits : sociologie politique de l'international,* Paris : L'Harmattan, août 2004, n°53, p.145.

[10] OCQUETEAU Frédéric, « La « sécurité globale », une réponse à la menace terroriste ? », *in* « L'État face aux risques », *Regards sur l'actualité,* Paris : La Documentation Française, février 2007, p. 57.

en part de fenêtres. Dans la tour est placé un surveillant et dans chaque cellule est enfermé un individu. Cette structure divise la foule des détenus et permet une surveillance efficace : le détenu se sait surveillé mais ne peut constater cette surveillance[11]. Ce qui ne peut être s'agissant des individus connectés au réseau, qui ne peuvent être tenus dans l'ignorance des régimes de contrôles qui pèsent sur eux.

5. **L'utopie d'un internet dit « Libre ».** Toutefois cette exigence de liberté et de transparence au profit des internautes n'équivaut pas à requérir de l'internet qu'il soit « Libre ». Cette expression d'un « Internet libre » est souvent employée quand il est question de l'action des pouvoirs publics sur le réseau ; elle est associée à l'adjectif « neutre » sans que l'on comprenne vraiment ce que cette neutralité recouvre pour ceux qui l'utilisent à cet endroit. Leur raisonnement fait appel au contexte de la création du réseau et à la technicité de celui-ci.

Ainsi, à l'instar d'un *« sociologisme extrême* », pour reprendre une expression de Henri Battifol, qui a pu nier au juriste son utilité considérant que, *in fine,* seul le courant social conditionnait la production de la norme[12] ; un « technologisme » ambiant tend aujourd'hui à considérer comme une illusion la capacité de décision des pouvoirs publics et du juriste quant à l'encadrement du réseau et de ses usages. Les techniciens considèrent en effet que l'effort de systématisation technique qui a été opéré pour mettre en œuvre le réseau des réseaux neutralise toute superposition d'un autre système de règles contraignantes. Le rôle du juriste est minimisé dès lors que l'objet à encadrer est déjà techniquement structuré. Cette position est critiquable en ce qu'elle opère un glissement bien trop rapide entre la spontanéité du réseau qui impose des usages et qui porte en lui ses futures avancées et la spontanéité de la norme qui nécessairement devrait en découler.

L'expression d'un internet dit « libre » ne peut ressortir que de prétentions libertaires. Le réseau doit être gouverné. La problématique juridique est de savoir comment envisager la cohérence des intérêts à protéger sur le réseau et organiser un système de règles efficaces. L'écueil à cet endroit est que cette réflexion semble se réduire aujourd'hui à la délimitation de nouveaux droits dits « fondamentaux ».

---

[11] Dès lors comme le souligne Foucault : « *De là, l'effet majeur du Panoptique : induire chez le détenu un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir. Faire que la surveillance soit permanente dans ses effets, même si elle est discontinue dans son exercice ; que cet appareil architectural soit une machine à créer et à soutenir un rapport de pouvoir indépendant de celui qui l'exerce ; bref que les détenus soient pris dans une situation de pouvoir dont ils sont eux-mêmes porteurs ».* V. : FOUCAULT M., *Surveiller et Punir, naissance de la prison,* Paris : Gallimard (*tel),* 1975, (impression 20 janvier 2007, p. 234).

[12] BATIFFOL Henri, «Droit comparé, droit international privé et théorie générale du droit », *in* BATIFFOL Henri, *Choix d'articles rassemblés par ses amis,* PARIS : L.G.D.J., 1976, p.346.

6. **Une nouvelle génération de droits de l'Homme.** Dès les prémices de l'informatique, l'enjeu de son encadrement est fortement ressenti. Au milieu des années 70, l'informatique se démocratise, notamment dans les administrations ; la centralisation et le traitement automatique d'informations inquiètent[13]. Plusieurs États européens[14] se dotent d'une législation spécifique dite « *Informatique et Libertés* », c'est-à-dire venant encadrer les usages de cette nouvelle technique qui doit tout à la fois respecter les libertés de l'individu et permettre le développement de la technique et de l'essor économique qu'elle génère[15].

Ces préoccupations viennent se fondre dans ce qui est appelée la troisième génération des droits de l'Homme. Très justement, en 1994, dans la première édition de son ouvrage, *Philosophie politique*, Nicolas Tanzer explique que, dans cette rubrique se trouvent en premier lieu : « *les droits à l'affirmation et à la protection du citoyen dans sa vie quotidienne, en matière de secret contre les risques que constituent les procédés informatique notamment. Par là, ces droits sont une réactualisation des droits de l'homme de la première génération constitutifs des libertés publiques en fonction des impératifs et des risques spécifiques des sociétés modernes* »[16].

Or cette protection de libertés séculairement garanties à l'individu eu égard à un objet nouveau, grâce à la mise en œuvre de lois spéciales, répondant à des risques délimités, ne s'envisage plus comme telle aujourd'hui. Alors que l'informatique a fait place au réseau, a émergé un droit pour l'individu à la protection de ses données

[13] En témoigne, le scandale du fichier S.A.F.A.R.I. pour Système Automatisé pour les Fichiers administratifs et le Répertoire des individus. La centralisation des données que ce dernier opère grâce au numéro national d'identité, dénoncé dans un article du journal *Le Monde*, au titre évocateur « Safari ou la chasse aux français » (de Philippe Boucher, paru le 21 mars 1974), accéléra en France, la réflexion autour d'une législation spécifique aux traitements de données par l'informatique.

[14] La Suède se dote d'une législation Informatique et Libertés le 11 mai 1973, l'Allemagne le 10 novembre 1976. Le Portugal, l'Espagne et l'Autriche ont respectivement introduit, en 1976 et 1978, la protection des données personnelles dans leur constitution. La France adopte la « *Loi relative à l'informatique, aux fichiers et aux libertés* », le 6 janvier 1978. La Grande-Bretagne vote le « *Data protection act*» en 1984.

[15] . Il faudra attendre 1995 pour qu'une directive communautaire vienne harmoniser les législations des États membres en matière de protection des données pour permettre une meilleure circulation de celles-ci. V. : Directive 1995/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre-circulation de ces données* », JO L281 du 23.11.1995, p.31. Cette directive est transposée en droit français par la loi du 6 août 2004 qui modifie dans son ensemble mais n'abroge pas la loi Informatique et Libertés du 6 janvier 1978. V. : Loi n°2004-801 du 6 Août 2004, « relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique et aux libertés », JORF du 7 Août 2004, texte 2 sur 92.

S'agissant des autres instruments régionaux : Le Conseil de l'Europe adopte en 1981 la Convention dite « STE108 ». V. : « *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* », Conseil de l'Europe, Strasbourg, 28.I.1981 ; l'OCDE adopte en 1985 la « *Déclaration sur les flux transfrontières de données* » et en 1988 « *La Déclaration relative à la protection de la vie privée sur les réseaux* » de 1988. V. *Les lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Paris, OCDE 2001.

[16] TANZER Nicolas, *Philosophie politique*, Paris : P.U.F., 1994 (1ère éd.), p.74.

personnelles ; parfois qualifié, sous la dénomination d'« *Habeas Data* »[17], de droit de l'Homme de la 4ème génération.

7. **La rhétorique du droit à la protection des données personnelles.** Formellement, le « droit à » la protection de ses données personnelles n'est consacré que par la Charte européenne des droits fondamentaux, adoptée le 7 décembre 2000, qui, dans son article 8, énonce « *Toute personne a droit à la protection des données à caractère personnel la concernant* »[18]. Le Règlement Général sur la Protection des Données (RGPD), adopté en avril 2016 et entré en vigueur le 25 mai 2018, indique, pour sa part, dans son premier article, au deuxième point, que : « *Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel* »[19]. La défense des libertés individuelles, et notamment de la vie privée, se fond ainsi dans un nouveau « droit à »[20] de plus en plus affirmé dans la vie quotidienne.

L'affirmation d'un tel droit n'est pas critiquable en soi dès lors que le mouvement de subjectivisation du droit répond à une inclination naturelle de l'homme vivant en société et qu'il vient ici incarner une exigence démocratique nouvelle. Le professeur Cornu rappelle « *l'assise populaire* » des droits subjectifs et « *l'instinct possessif* »[21] qui est sans doute à la racine d'une telle prérogative. Le Doyen Carbonnier affirme pour sa part que : « *La vérité est que le droit subjectif, en dépit de son individualisme, est très sociologique. Pour que le droit objectif soit intensément présent dans la société, rien de tel que de l'incarner, donc de le subjectiviser* »[22]. La rhétorique de tout « droit à » qui consiste en un effet d'annonce et qui est nécessaire à l'imprégnation réciproque par le droit et la société d'une problématique réelle n'est pas critiquée ici.

---

[17] Une expression employée en référence à l'« *habeas corpus* » britannique, non pas toutefois envisagé dans sa signification originelle et stricte qui renvoie au fait de ne pouvoir être emprisonné arbitrairement, mais en référence plus généralement à cette notion de maîtrise de l'individu sur son corps, et donc en l'espèce sur ses données.

[18] Cette charte est, depuis le traité de Lisbonne qui est entré en vigueur le 1er décembre 2009, un instrument juridique contraignant pour les Etats membres au même titre que les traités (V. article 6 du Traité sur l'Union européenne (2012), JOUE du 26/10/2012, C326/1-407).

[19] Règlement (UE) 2016/679, du Parlement européen et du Conseil du 27 avril 2016 « *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre-circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données),* JOUE, 4.5.2016, L119/1-87.

[20] Sur le développement des « droit à » : v. COHEN Dany, « Le droit à… », *in L'avenir du droit, Mélanges en l'honneur de François Terré,* Paris : Dalloz, 1999, p.393. Pour une classification des nouveaux « droits à » : v. PICHARD Marc, *Le droit à, étude de législation française,* Paris : Economica, 2006 (Recherches juridiques). Sur la dissociation de la protection des données personnelles du droit au respect de la vie privée : V. DREYER E., « La fonction des droits fondamentaux dans l'ordre juridique », *D. 2006,* n°11, p.748.

[21] CORNU Gérard, *Droit civil, Introduction au droit,* 13ème éd., Paris : Montchrestien, 2007 (Domat, droit privé), n°36.

[22] CARBONNIER Jean, *Flexible droit,* 10ème éd., Paris : 2001, L.G.D.J, p. 197 (*in* Chapitre unique : « Théorie sociologique du droit subjectif »).

Ce qui est critiquable c'est que la formulation de ce nouveau « droit à » annihile tout effort de construction et de visibilité d'un régime fondé sur la délimitation des risques eu égard à la réalité du réseau.

8. **La crise des droits de l'Homme et des libertés publiques**. La formulation même d'un « *droit à* » « *une protection* » est redondante et démontre l'ambigüité de cet objectif qui n'en est pas un s'il entend garantir une protection avant de définir un espace de liberté. La construction du droit est inversée : un objectif ne guide pas la mise en œuvre d'une protection, il s'en extrait. Dès lors, on ne saurait nier qu'il est motivé par « *une réalité objective parce que collective* »[23] mais son essence de droit subjectif se doit d'être questionnée.

En 1996, Jean Morange soulignait qu'il fallait distinguer clairement la crise des libertés publiques « *de ce que plus fréquemment on désigne par crise des libertés ou crise des droits de l'homme* »[24]. Il est pertinent de souligner cette distinction dont les enjeux se retrouvent dans l'émergence d'un « *droit à la protection de ses données personnelles* », exemple topique, à la fois de la « *pulvérisation du droit en droits subjectifs* »[25] et de la *« floraison de la fondamentalité »*[26]. La protection des libertés de l'individu ne semble aujourd'hui effective que par le biais de la formulation d'un « droit à » qui concrétise l'exigence d'un individu et qu'il convient d'élever au plus haut rang dans la hiérarchie des normes alors que la loi est en crise. Ainsi le droit à la protection des données personnelles ne définit pas une exigence de liberté, ménageant un espace possible pour une règlementation. Ce « droit à » fait de l'objet du régime l'objectif de la protection : il faut protéger les données et consacrer dès lors « l'appartenance-maîtrise », pour citer Dabin, de l'individu sur celles-ci.

Or cette cristallisation d'objets nouveaux à protéger dans des droits fondamentaux enserre l'approche technique de leur encadrement. La critique qui fut celle de Gény à l'égard de « l'école du droit naturel » peut être reprise ici. Il convient de revenir à une approche pragmatique des nouvelles technologies, qui seule permettra de considérer les objectifs à atteindre qui sont multiples et doivent être délimités.

---

[23] Le doyen Carbonnier souligne les deux phénomènes qui ont contribué à pousser les droits subjectifs au premier plan : l'expansion de l'idéologie des droits de l'Homme et l'engouement pour la psychologie au détriment de la sociologie. Il affirme que : « *Il s'en est suivi un changement dans la manière de légiférer : le législateur aime partir d'un droit fondamental de l'individu plutôt que d'une réalité objective parce que collective* ». V. : CARBONNIER Jean, *Droit civil Introduction*. 27éd. refondue Paris : P.U.F, 2002, (Thémis Droit privé), n° 162, p.325.

[24] MORANGE Jean « La crise de la notion de liberté publique » *in L'unité du droit, Mélanges en hommage à Roland Drago*, Paris : Economica, 1996, p.91.

[25] CARBONNIER Jean, *Droit et passion du droit sous la Vème République*, Paris : Flammarion, 1996, (Champs essais), p.121, III « La pulvérisation du droit en droits subjectifs ».

[26] BURGORGUE-LARSEN Laurence, « Libertés publique(s) et droit fondamental », *in L'influence du droit européen sur les catégories de droit public*, Jean-Bernard AUBY (*dir.*), Paris : Dalloz, 2010, (coll. Thèmes et commentaires), p.286

9. **Le changement de paradigme : dépasser l'affirmation d'un « droit à »**. L'affirmation d'un « droit à » est un procédé intellectuel qui conceptualise un objet de protection. Or il n'est pas, à la différence des sciences exactes, de vérité juridique absolue[27]. Ainsi, il faut tester la capacité d'action d'un concept sur le réel pour en déduire son bien-fondé, et dès lors, *de facto*, considérer qu'il puisse évoluer dans le temps. La méthode de Gény invite ainsi à découvrir la réalité des faits afin d'appréhender les *desiderata*[28] essentiels qui s'en dégagent. Ceux-ci envisagés comme des objectifs à atteindre ont pour vocation de « *civiliser le droit positif* »[29] et non de l'assujettir. Ce but à atteindre laisse une marge de manœuvre quant au dispositif à mettre en œuvre ; l'élaboration et l'interprétation du droit positif font l'objet d'une technique[30].

Ainsi il convient de ressentir les exigences essentielles qui se dégagent de la réalité du réseau pour apprécier la nécessité éventuelle d'un droit subjectif qui s'élèvera dans la hiérarchie des normes. Et ne pas faire l'inverse : partir d'un droit subjectif que l'opinion, guidée en l'occurrence ici par la peur naturelle de l'homme envers la machine, juge fondamental pour adopter un corpus de règle dont la cohésion n'a pas été réfléchie et peut donc être discutée. Le juriste ne verra alors dans cette protection rien de tangible et, recours recevable, arguera du rôle de la jurisprudence pour transposer ces nouveaux concepts à la réalité. Cela n'est pas tout à fait satisfaisant et le propre de cette étude est de prendre le recul nécessaire pour trouver une cohésion à un corps de règles, qui malléable, viendra encadrer efficacement l'utilisation du réseau.

Il faut ainsi appréhender un nouvel état de fait, pour ensuite réfléchir au possible épanouissement des libertés déjà garanties à l'individu eu égard à cette réalité nouvelle.

---

[27] GAUTIER Pierre-Yves, «Réflexions sur François Gény, l'actualité méthodologique de *Science et technique », in La pensée de François Gény, (*O.CACHARD, F-X LICARI, F. LORMANT *dir.*) Paris : Dalloz, 2013, (Thèmes et commentaires, Actes), p.51.

[28] Ce terme est utilisé par Raymond Saleilles dans la préface qu'il fait de l'ouvrage de Gény. V. : GENY François, *Méthode d'interprétation et sources en droit privé positif : essai critique*, 2ème éd., Paris : LGDJ, 1919. (Publié une première fois en 1899), Tome 1, préface p. XVIII.

[29] SERIAUX Alain, entrée le « Le droit naturel » *in Dictionnaire de la culture juridique,* ALLAND Denis et Stéphane RIALS (*dir.*), Paris : Lamy, P.U.F., (Quadrige-Dicos Poche) 2003, p.511.

[30] Toutefois, de la même manière que la philosophie de « l'École du droit naturel » a accouché du positivisme légaliste, les objectifs à poursuivre envisagés comme des « *étoiles directrices* » par le Doyen nancéien, semblent devenus des concepts supérieurs contraignants, qui enserrent de manière critiquable la création d'une protection adéquate aux dangers qu'ils entendent dénoncer. Ainsi l'opposition de Gény à l'encontre de la technique exégétique pourrait être transposée aujourd'hui à l'égard du recours aux droits fondamentaux. Face à une réalité nouvelle, le seul axe de réflexion, ne peut être celui de l'affirmation d'un « droit fondamental ». Il convient d'être pragmatique. V. : FRYDMAN Benoît « Le projet scientifique de François Gény », in *François Gény, mythe et réalités 1899-1999 centenaire de Méthode d'interprétation en droit privé positif, essai critique*. THOMASSET C., VANDERLINDEN J et P. JESTAZ (*dir.),* Les éditions Yvon Blais, Dalloz, Bruylant Bruxelles, 2000 (thèmes et commentaires, études), p. 218.

10. **La compréhension de la technique du réseau.** La première étape de tout raisonnement juridique est de comprendre les faits. Le Doyen Gény souligne que « *plus on connaîtra la réalité elle-même, par l'effort d'une intuition directe, dégagée des subtilités d'une analyse raffinée, mieux on aura de chances de découvrir les règles capables de diriger la vie* »[31].

Toutefois, alors que l'organisation du réseau a été pensée et est techniquement complexe, le rapport du juriste avec l'objet qu'il cherche à encadrer est bouleversé. Ce dernier n'est plus à l'intérieur du système mais l'observe de l'extérieur. Le point de départ de la réflexion doit consister en un effort pour comprendre la réalité alors que le juriste ne peut se fier à son seul ressenti à ce niveau. En effet, la dématérialisation de tous les procédés, leur nouveauté et leur technicité empêchent la compréhension immédiate de tous les tenants et aboutissants d'une action sur le réseau. Une compréhension peut résulter de l'expérience et d'un processus d'analogie mais l'empirisme de la méthode couplée à la nouveauté du réseau limite de beaucoup l'analyse.

Cela étant, cette étude a cherché à aborder ces recherches sur la technique du réseau avec enthousiasme en suivant tout de même cette intuition dont parle Gény. Cet exercice s'est avéré fructueux et gratifiant ; la logique du juriste rencontrant celle des informaticiens, par ailleurs toujours très didactiques dans leurs explications. Il apparait que le réseau peut être envisagé comme un nouvel espace qui invite à réinterpréter les libertés individuelles séculairement garanties à l'Homme, non pas seulement intellectuelles mais bien aussi physiques.

11. **La difficile qualification des problématiques soulevées par le réseau**. La lecture des plans adoptés par divers manuels de libertés publiques et droits fondamentaux fait apparaître la difficulté de qualification des problématiques diverses que génère l'usage du réseau. La solution est alors souvent de présenter celles-ci dans un paragraphe ou une partie dense qui ressemble à un catalogue.

Le professeur de droit public Henri Oberdorff traite de la « *la liberté individuelle et des développements de la société numérique* » et aborde, entre autres, dans ce paragraphe le développement de la liberté de communication, l'e-gouvernement, le

[31] GENY François, *Des droits sur les lettres missives, étudiés principalement en vue du système postal français*, Recueil Sirey : Paris, 1911, avant-propos p.XII.

traçage électronique, la fracture numérique, la cybercriminalité et le droit à l'oubli[32]. Le professeur de droit public Xavier Bioz étudie ces problématiques dans un paragraphe intitulé « *Liberté d'expression sur Internet* » qui en quatorze points couvre notamment, la liberté de communication en ligne, le droit d'accéder à internet, les transferts internationaux de données, les cookies et les spams[33]. Ainsi les développements de l'internet sont parfois rattachés à la notion de liberté individuelle ou à celle de liberté d'expression. Les interrogations autour des libertés à sauvegarder sur le réseau voisinent avec la mention de problématiques précises et techniques, telle que celles des cookies sans qu'aucun lien ne soit fait entre les deux. Pour qu'une qualification effective des problématiques puisse s'opérer, il convient d'appréhender la réalité de l'environnement nouveau, et de distinguer à ce niveau des spécificités qui puissent ordonner les problématiques qu'il fait naître.

Une qualification est possible si l'on distingue la production de données nécessaires à l'échange de contenus sur le réseau d'une part, et la mise en ligne de données qui viennent constituer ces contenus disponibles d'autre part. En effet, le réseau est à la fois un nouveau moyen de communication et un nouveau média. Cette distinction conduit à une première qualification des objectifs à atteindre qui prend pour critère celui de l'objet du droit ou de la liberté à sauvegarder. Cette distinction suivant l'objet de la liberté n'est pas jugée comme la plus opérante alors qu'elle peut donner lieu à des interférences. La structure du réseau permet toutefois une qualification efficace qui distingue le nécessaire épanouissement des libertés intellectuelles eu égard à ce nouveau média qu'est le web (en français « la Toile »)[34] et le nécessaire épanouissement des libertés physiques eu égard à ce nouveau moyen de communication qu'est le réseau internet.

12. **L'enjeu des « libertés de communication ».** Est reprise ici la formule du professeur Jacques Georgel, et de son ouvrage « Les libertés de communication »[35]. Ce professeur de droit public indique, dans son introduction, que la liberté de communication présente deux faces : la liberté de « communication physique » et la liberté de « communication mentale ». La première, dit-il, correspond au déplacement du corps dans l'espace, la seconde au contact

[32] OBERDORFF Henri, *Droits de l'homme et libertés fondamentales,* 3ème éd., Paris : L.G.D.J, Lextenso éditions (manuel), 2011, p. 381.

[33] BIOY Xavier, *Droits fondamentaux et libertés publiques*, Paris : Montchrestien, Lextenso éditions, 2013 (LMD édition, Collection cours, *dir.* B. Beignier), n °1185, p.428.

[34] Il est décidé dans cette étude d'utiliser l'abréviation web, provenant de l'expression World Wide Web, désormais bien établie et d'usage courant en français. Le choix est fait d'utiliser une minuscule, renvoyant à celle aussi choisie pour le terme « internet » dont l'usage est tel aujourd'hui qu'il ne s'agit plus de les considérer comme des noms propres.

[35] GEORGEL Jacques, *Les libertés de communication,* Paris : Dalloz (Connaissance du droit, droit public), 1996.

mental entre deux personnes via les télécommunications. Le sous-titre de son ouvrage précise qu'il va traiter du contrôle d'identité, des écoutes téléphoniques et de la vidéosurveillance. En quatrième de couverture, il exclut de son champ d'étude la liberté de communication entendue comme la liberté permise par les médias.

Cette approche qui met au pluriel la formule « libertés de communication », qui inclut dans cette communication, la circulation physique de l'individu sur le territoire et qui exclut l'expression permise par les médias, nous paraît très pertinente eu égard au réseau internet. En effet, il faut souscrire au raisonnement du professeur Georgel qui en rattachant à la communication le déplacement physique de l'individu souligne avec profit cette distinction à faire entre la diffusion des idées à un public, et la communication de la personne avec un semblable soit en se déplaçant vers lui, soit en correspondant avec lui. Ces deux types de communication renvoient en effet à des problématiques différentes qui ont trait pour la diffusion d'idées, à la sauvegarde de la liberté d'expression et pour la mise en relation avec autrui à la sauvegarde des libertés dites de la personne physique .

13. **La protection des libertés de la personne physique.** Dans son manuel de libertés fondamentales, le professeur Morange reprend les propos du Doyen Hauriou qui rappelle que : « *Historiquement, le statut de l'homme libre garantissant sa liberté physique et son droit de propriété, a été élaboré avant les libertés de conscience ou de la pensée. Dans cette perspective, la liberté de conscience viendrait couronner la reconnaissance de la liberté d'aller et venir, du droit à la sûreté et de la protection de la vie privée* »[36].

Il doit en aller de même sur le réseau. Il faut réfléchir à ce qui était nommé, dans les manuels de libertés publiques, notamment celui de Georges Burdeau[37], « *les libertés de la personne physique* » ; celles-ci étaient différenciées de la liberté de la pensée. Elles renvoyaient traditionnellement à la sûreté individuelle, entendue comme le fait pour un individu de ne pouvoir être arbitrairement détenu, à la liberté d'aller-et-venir et à la liberté de l'intimité. Cette dernière relevait alors seulement d'une conception objective visant la protection du domicile et des correspondances ; elle était encore matériellement rattachée à la liberté individuelle visée par l'article 66 de la Constitution. La liberté de la pensée pour sa part faisait d'abord référence dans des temps plus anciens, non pas à la liberté d'expression en général mais à la liberté de la presse et à l'encadrement de cette industrie.

[36] MORANGE Jean, *Les libertés publiques*, 8ème éd., Paris : P.U.F., 2007 (coll. QSJ), p.46.
[37] BURDEAU Georges, *Les libertés publiques*, 4ème éd., Paris : Librairie générale de droit et de jurisprudence, 1972.

Les libertés de la personne physique sont indissociables des libertés intellectuelles. La difficulté toutefois est que les enjeux visant les libertés de la personne physique ne sont pas considérés sur le réseau internet. Ainsi la réflexion autour des libertés fondamentales vise d'une part la sauvegarde de la liberté d'expression envisagée plus largement comme la liberté de communiquer et de recevoir des informations, dont les modalités ont subi une véritable révolution alors que chacun peut aujourd'hui accéder à une audience via le web ; et d'autre part, alors que toute connexion et choix de connexion sont matérialisés par une donnée, la protection de l'intimité de l'internaute n'est envisagée qu'à travers le prisme de la protection des données personnelles et de son champ d'application élargi.

Dès lors, les raisonnements apparaissent parfois spécieux alors que les problématiques ne répondent plus d'un système de libertés éprouvé qui ménage tout à la fois des garanties contre l'arbitraire du pouvoir et organise le régime de la liberté d'expression.

14. **L'objectif de défense de l'internaute contre l'arbitraire du pouvoir**. L'étude propose de réinterpréter ces libertés dites de la personne physique. Le réseau est, avant que d'être un nouveau média grâce à son application web, un nouveau moyen de communication qui doit respecter la sûreté de l'internaute au sens large.

Comme l'énoncent les professeurs Rivero et Moutouh dans leur manuel de libertés publiques : « *la notion de sûreté est beaucoup plus large : au delà même de la privation de liberté physique, elle condamne toute forme arbitraire de répression. L'objet de la sûreté est donc la sécurité juridique de l'individu face au pouvoir. Par là, elle constitue également une protection avancée de toutes les autres libertés. Elle aussi est une liberté fondamentale, qui garantit les autres* »[38]. Les auteurs poursuivent en distinguant cette sécurité juridique de la sécurité physique. Ils affirment qu'à cette sécurité juridique peuvent être rattachées aussi « *car il s'agit d'une protection avancée contre toutes les formes d'arbitraire, les mesures prises pour prévenir les dangers auxquels la concentration des informations individuelles, notamment par le biais des nouvelles technologies expose les particuliers* »[39].

Cette analyse sied à notre approche qui envisage la protection des libertés de la personne physique sur le réseau. La liberté individuelle, au singulier, visant, au sens

[38] RIVERO Jean, MOUTOUH Hugues, *Libertés publiques,* Tome I, 9ème éd., Paris : P.U.F. Droit (Thémis, droit public), p. 17.

[39] *Ibid.*

strict, les arrestations et les détentions, et la liberté d'aller et venir de l'individu doivent être réinterprétées sur le réseau. Deux nouvelles libertés doivent être consacrées : la liberté d'accès au réseau et la liberté de naviguer sur le web. Celles-ci définies, peuvent alors être envisagé les principes devant encadrer la collecte des données produites automatiquement par chaque connexion au réseau. Ainsi les problématiques visant la liberté d'expression sur le web et notamment les régimes de responsabilité des différents acteurs du réseau, et celles considérant l'encadrement des informations mises en ligne par les internautes, qui questionnent notamment aujourd'hui le droit à l'oubli, ne sont pas traitées dans cette étude.

15. **La mise en œuvre de libertés publiques**. Cette thèse envisage le réseau internet comme un nouvel espace qui invite à réinterpréter les libertés qui sont garanties à l'individu dans le monde physique. Au titre des libertés fondamentales, sont protégées la liberté individuelle, entendue comme le fait de ne pouvoir être arbitrairement détenu, et la liberté d'aller et venir de tout citoyen. Il doit en aller de même sur le réseau. Deux libertés doivent être consacrées eu égard à l'usage du réseau : la liberté d'accès au réseau et la liberté de naviguer sur le web.

Elles ne s'envisagent pas comme de nouveaux « droit à », tel un « *droit à l'accès* » ou un « *droit à un internet libre* ». Ces formulations, souvent employées, sont maladroites en ce qu'elles ne peuvent se détacher du contexte politique qui les a vu naître et semblent renvoyer à des créances indéfinies de l'individu face à l'État. La logique défendue ici est celle de libertés publiques : l'affirmation d'une liberté renvoie à un régime objectif de principes légaux qui la mettent en œuvre. Le Doyen Favoreu rappelle que, outre leurs différences de niveaux normatifs, libertés publiques et droits fondamentaux font l'objet d'un « *mode opératoire distinct : les libertés publiques opèrent comme des limitations des prérogatives du pouvoir exécutif et notamment de la police en provoquant une définition concrète du régime de certaines activités ; tandis que les droits fondamentaux, sont, en quelque sorte, des créateurs de « réflexe » ou des « germes » ou encore des « sources de rayonnement » destinés à faire évoluer les concepts de base des diverses matières concernées* »[40].

L'objet de cette étude est de considérer dans quelle mesure le pouvoir exécutif peut gouverner le réseau tout en ménageant la liberté d'accès et la liberté de naviguer de

[40] FAVOREU Louis, *et al.*, *Droit des libertés fondamentales*, 6ème éd., Paris : Dalloz (Précis, droit public, science politique), Introduction, p. XVI.

l'internaute. Ce qui invite également à s'interroger sur le pouvoir des fournisseurs d'accès au réseau et des entreprises du web.

16. **Le respect des libertés individuelles sur le réseau internet.** Ainsi, dans un premier temps, le contenu de la liberté d'accès au réseau et le contenu de la liberté de naviguer sur le web doivent être définis (***Première partie)***. Dès lors, dans un second temps il sera vu que ces libertés n'ont de sens que si deux principes sont mis en œuvre : l'internaute doit être assuré qu'il accède au réseau anonymement et qu'il ne fait pas l'objet d'une surveillance arbitraire lorsqu'il navigue sur le web **(*Deuxième partie)*.**

Première partie : Le contenu des libertés individuelles à sauvegarder sur le réseau

Deuxième partie : Les principes à mettre en œuvre pour sauvegarder ces libertés

Première partie. Le contenu des libertés individuelles à sauvegarder sur le réseau internet

17. **Les libertés de la personne physique sur ce nouvel espace qu'est internet.** Un individu derrière son écran a, grâce à sa connexion au réseau internet, accès à une masse d'informations incalculable[41] et à un nombre de services toujours plus croissant ; le web étant désormais qualifié d'« applicatif »[42]. Or comme le rappelle le philosophe et historien des techniques Michel Serres, ce qui distingue le réseau des anciens moyens de communication n'est pas la masse d'informations à disposition, ni la vitesse de transmission, ni la notion de mise en réseau, mais le rapport à l'espace[43].

En effet, l'individu qui communique sur le réseau n'est plus lié à un point figé de l'espace métrique tel que celui d'une ligne fixe de téléphone ; par ailleurs, il n'est plus limité par une contrainte physique de déplacement pour accéder à l'information qu'il souhaite obtenir. Ainsi à l'individu, situé n'importe où sur le territoire, viennent l'ensemble des contenus et des services du web. Le rapport à l'espace sur le réseau internet n'est donc plus métrique. La question est alors de considérer comment cet espace peut être gouverné.

Un parallèle peut être fait entre les libertés à sauvegarder dans le monde physique, lieu de circulation des hommes et les libertés à sauvegarder sur le réseau, lieu de transmission de données. Ainsi dans le monde physique, l'État peut agir sur l'individu, l'enfermer et lui interdire tout déplacement, ou limiter et règlementer celui-ci. Ces possibilités sont les mêmes sur le réseau, à la différence que ce n'est plus l'individu qui est contraint, mais la structure même du réseau. Ainsi sur le réseau, l'État peut agir aux deux points de la communication. D'une part il peut couper l'accès au

[41] « Si nous savons combien il y a d'internautes dans le monde – environ 2 milliards – et de sites web – plus de 200 millions – le nombre de pages reste inconnu. Bien qu'estimé à environ 1 billion (1000 milliards) par Kevin Kelly de Wired » V. : SANYAS N., « Combien de pages web y-a-t-il sur internet ? », article mis en ligne le 15 septembre 2011 sur le site : www.pcinpact.com

[42] Comme le souligne Pascal Francq, ingénieur, le Web initialement pensé comme « *un simple support de mise en ligne hypertexte, s'est progressivement mué en une structure applicative proposant une multitude de services en ligne (gestion de courriels, sites Web personnels, consultation de cartes, etc.)* ». V. : FRANCQ P., *Internet, Tome 1 : La construction d'un mythe,* Bruxelles : E.M.E (Editions Modulaires Européennes) (Techno, logos, ЄҬ Polis), 2011, p.99.

[43] « Les nouvelles technologies, que nous apportent-elles ? », conférence de Michel Serres, enregistrée à l'École Polytechnique le 1er décembre 2005, faisant partie du cycle *Culture Web*, coordonné par Serge Abiteboul, dans le cadre des Thématiques INRIA. Disponible au format mp3 sur le site : interstices.info, rubrique « débattre ».

réseau mis à disposition de l'internaute, et lui interdire ainsi tout usage du réseau quel qu'il soit. D'autre part, il peut, à l'endroit des serveurs stockant les sites web, opérer un blocage s'agissant de certains d'entre eux ; l'internaute ne peut alors plus les consulter.

18. **La sauvegarde de la liberté d'accès au réseau et de la liberté de naviguer sur le web.** Or il faut s'interroger sur les conditions de la mise en œuvre d'une telle coupure d'accès qui peut donc, en suivant l'analogie établie par cette étude, s'apparenter à une mesure privative de liberté. De la même manière le blocage de sites peut être considéré comme une mesure restrictive de la liberté de l'internaute de naviguer sur le web. Or cette logique de privation ou de restriction doit être encadrée et amène à considérer dans un premier lieu le caractère fondamental de deux libertés : celle d'accès au réseau, et celle de naviguer sur le web.

Ainsi il faut envisager dans un premier temps le régime qui permet de mettre en œuvre la liberté d'accès au réseau **(Titre I),** puis dans un second temps, celui qui permet de mettre en œuvre la liberté de naviguer sur le web **(Titre II)**.

Titre I. La liberté d'accès au réseau
Titre II. La liberté de naviguer sur le web

TITRE I. LA LIBERTE D'ACCES AU RESEAU

19. **La peur de reconnaître en soi une liberté d'accès au réseau**. Si la valeur fondamentale de l'accès au réseau est aujourd'hui reconnue par les autorités, cette affirmation ne conduit pas à la consécration d'une nouvelle liberté publique, ce qu'il faut regretter. Ainsi dans le cadre de la révision du Paquet télécom, l'Union européenne affirme que « *Étant donné que l'internet est essentiel pour l'éducation et pour l'exercice pratique de la liberté d'expression et l'accès à l'information, toute restriction imposée à l'exercice de ces droits fondamentaux devrait être conforme à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. La Commission devrait lancer une vaste consultation publique à ce sujet.* »[44]. Toutefois le Parlement européen dans une recommandation à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur internet utilise le conditionnel : « *Si l'accès à internet était considéré comme un droit fondamental dans l'Union* […] »[45].

Dans sa décision du 10 juin 2009 (Loi favorisant la diffusion et la protection de la création sur Internet)[46], le Conseil constitutionnel après avoir rappelé l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789[47] affirme que « *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 des opinions, ce droit implique d'accéder à ces services* »[48]. Cette annexion à la liberté de communication qui, sur le fondement de l'article 11 est confondue avec la liberté d'expression, est maladroite en ce qu'elle ne dissocie pas l'épanouissement des libertés intellectuelles et des libertés physiques permises par le réseau.

---

[44] Considérant 4 de la Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009, « *modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques* », JOUE du 18/12/2009, L337/37-69.

[45] Recommandation du Parlement européen du 26 mars 2009 à l'intention du Conseil sur le renforcement de la sécurité et des libertés fondamentales sur Internet (2008/2160(INI)).

[46] Conseil constitutionnel, décision n°2009-580DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, JORF du 13 juin 2009, p.9675.

[47] « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi* », Déclaration des Droits de l'Homme et du Citoyen de 1789, article 11.

[48] Conseil constitutionnel, décision n°2009-580DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, JORF du 13 juin 2009, p.9675, considérant n°12.

En 2015, dans le cadre de l'adoption de la loi pour une République numérique, un amendement est proposé qui consacre l'accès au réseau en ces termes : « *Tout individu a le droit d'accéder à Internet dans des conditions d'égalité, suivant des modalités technologiquement adéquates et actualisées qui lèvent tout obstacles d'ordre économique et social* »[49]. Dans l'exposé sommaire qui est fait de cet amendement, il est affirmé que celui-ci « *vise à garantir à chacun un droit de caractère général et absolu à être connecté* ». Il est fait mention de la décision du Conseil constitutionnel du 10 juin 2009 ; il est souligné qu'internet est «*un élément quasi-incontournable du lien social, voire, dans certains cas, le lieu d'exercice des droits fondamentaux* »[50].

Jugé purement déclaratif, l'amendement est retiré[51]. Il faut le regretter alors même que si la formulation d'un « *droit à* » « *de caractère général et absolu* » est à condamner, cette proposition avait le mérite de faire émerger le préalable nécessaire à une république numérique, la consécration d'une liberté d'accès au réseau. Cet amendement esquissait d'ailleurs, même si maladroitement, la nécessité d'un service public devant garantir cette liberté en faisant mention de l'égalité et de l'uniformisation des pratiques à mettre en œuvre.

20. **Analogie de la liberté d'accès avec la sûreté personnelle**. Ainsi ces positions qui font preuve d'une approche évolutive des libertés eu égard à l'existence du réseau mondial doivent être saluées. Toutefois, du fait de la peur d'un internet libertaire et d'un « droit à » non défini, le raisonnement n'est pas mené à son terme. Il faut affirmer que l'accès au réseau permet l'exercice paisible non pas de la seule liberté de communication et d'expression, mais bien de toutes les libertés et considérer alors que la liberté d'accès nécessite d'être reconnue préalablement à celles-ci. Elle doit être entourée d'une garantie supérieure à celle entourant l'exercice de chacune des libertés prises séparément.

Alors que le réseau peut être appréhendé comme un environnement nouveau permettant l'exercice de libertés déjà établies, une analogie peut intervenir pour délimiter les contours de cette nouvelle liberté publique. La possibilité d'accéder à ce nouvel environnement qui permet l'épanouissement de toutes les libertés reconnues à l'homme s'apparente à la sûreté de l'individu dans le monde physique. Ne pas

[49] Amendement n°274, amendements déposés sur le texte n°3399, Voir le dossier législatif « Economie : pour un République numérique » disponible sur le site de l'Assemblée nationale à cette adresse : http://www.assemblee-nationale.fr/14/dossiers/republique_numerique.asp

[50] *Ibid.*

[51] Assemblée nationale, XIVème législature, session ordinaire de 2015/2016, compte-rendu intégral, 2ème séance du mardi 19 janvier 2016. Voir le dossier législatif « Economie : pour un République numérique » disponible sur le site de l'Assemblée nationale à cette adresse : http://www.assemblee-nationale.fr/14/dossiers/republique_numerique.asp

permettre l'accès au réseau à un individu le prive des nouvelles modalités d'exercice de toutes ses libertés.

Cette approche qui pose l'accès au réseau comme une condition de l'exercice des libertés fonde le caractère fondamental de cette liberté, ce qui n'équivaut pas à en faire un droit ou une liberté absolu comme certains peuvent le craindre[52]. Aucun droit ou liberté ne peut être absolu dès lors que « *la liberté consiste à faire tout ce qui ne nuit pas à autrui* »[53]. Le caractère fondamental de l'accès au réseau, au sens de « fondement » des autres libertés, appelle simplement à un rapport de proportionnalité différent entre l'atteinte portée aux autres libertés et à autrui et la sanction qui va en découler eu égard à la privation de cette liberté de premier rang. Ce rapport doit être celui qui emporte la privation de liberté physique d'un individu[54].

21. **Plan.** Il convient ici d'éviter la formulation « droit à » l'accès qui est stigmatisée par une revendication forte. Cette revendication permet une prise de conscience et la tenue d'un débat nécessaire ; elle tend toutefois à faire planer le spectre d'un droit « à tout » qui renverrait à une créance indéfinie à la charge de l'Etat ou pire à un droit subjectif qui n'étant pas défini s'opposerait à toute limitation de l'usage du réseau.

L'accès au réseau est l'objet d'une nouvelle liberté publique. Cette liberté est fondée par sa délimitation qui conduit à définir les exigences d'un nouveau service public (***Chapitre 1er)***. Le caractère fondamental de l'accès au réseau doit être reconnu pour permettre la mise en œuvre d'un régime effectif visant la coupure d'accès au réseau (***Chapitre 2ème).***

---

[52] David El Sayegh, directeur général du SNEP (Syndicat National de l'Edition phonographique) qui critique en ces termes la décision du Conseil constitutionnel du 10 juin 2009 (Loi relative à la diffusion et à la protection de la création sur internet, 2009-580 DC) : « *Si dans sa décision le Conseil constitutionnel reconnaît l'accès à internet comme faisant partie de la liberté de communication, la reconnaissance d'une telle liberté ne revient pas à affirmer que l'accès à internet est un droit absolu auquel rien ne pourrait déroger, pas même le respect des droits de propriété littéraire et artistique* », EL SAYEGH David, « Le Conseil constitutionnel et la loi Création et Internet : une décision en trompe l'œil », *Légipresse*, n°263 Juillet/Août 2009, tribune p.97. Les cahiers du Conseil constitutionnel dans leur commentaire de la décision affirment bien que « *Affirmer la liberté d'accéder à Internet ne revient pas à garantir à chacun un droit de caractère général et absolu d'y être connecté*. », Commentaire de la décision n°2009-580 DC -10 juin 2009, Loi relative à la diffusion et à la protection de la création sur internet, 2009-580 DC, *Les cahiers du Conseil constitutionnel*, n°27, 2009, p. 101.

[53] Article 4 de la Déclaration des Droits de l'Homme et du Citoyen de 1789.

[54] Il est à noter que cette approche n'est pas celle adoptée par le Conseil d'État dans son rapport de l'année 2014 ; alors qu'il entend la liberté individuelle strictement comme le droit de ne pas faire l'objet d'un détention arbitraire et qu'il la distingue selon la jurisprudence établie du Conseil constitutionnel de la « *liberté personnelle, proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen* » qui est « *plus large et couvre le droit à la vie privée, l'inviolabilité du domicile, la liberté d'aller et venir et la liberté du mariage* ». Le rapport énonce ainsi que : « *Si le numérique ne peut par lui-même mettre en cause la liberté individuelle, ses utilisations à des fins de protection de la sécurité peuvent porter atteinte à la liberté personnelle* ». *V. « Le numérique et les droits fondamentaux* », étude annuelle 2014, *Les Rapports du Conseil d'État* (ancienne collection Étude et documents du Conseil d'État), p.110, (édité par la Documentation française et disponible à cette adresse : http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux).

Chapitre 1er. La délimitation de ce nouveau principe de liberté

Chapitre 2ème. La reconnaissance du caractère fondamental de ce nouveau principe

Chapitre 1er. La délimitation de ce nouveau principe de liberté

22. **Le constat d'un nouveau principe de liberté**. « *Un principe de liberté, ça se décrit peu, ça se constate* », ainsi M. le professeur Didier Truchet introduisait-il son chapitre portant sur « *La liberté de publier et ses limites*» issue de son cours de Master 2 « *Liberté d'expression, droit de la presse et de la communication audiovisuelle* »[55]. Le champ d'action permis par le réseau peut être immédiatement appréhendé par chacun et il ne s'agit pas de disserter sur les possibilités nouvelles qu'offre le réseau au risque alors d'établir un catalogue.

Il apparaît aujourd'hui que la mise en œuvre de l'accès au réseau témoigne du niveau de développement d'un État et de son dynamisme démocratique ; il revêt ainsi les enjeux d'un service qui doit être universellement garanti **(Section I).** Un tel service n'a de sens que si une fois l'accès établi, chaque connexion est traitée sans discriminations ce qui invite à s'interroger sur l'encadrement de l'activité des opérateurs de communications électroniques **(Section II).**

Section I. La mise en œuvre d'un service public universel d'accès au réseau

23. **La dématérialisation de toute activité.** Au début des années 2000, l'usage croissant de différents préfixes, tel le « e- » pour « électronique » [56], témoigne de la prégnance de l'usage du réseau dans tous les domaines. Se développent l' « e-commerce », le « e-business », le « e-learning », l' « e-governance », le « télétravail », la « télémédecine », la « cybercriminalité », la « cyberdéfense » ou encore la « cyberdémocratie ».

Toute activité tend à être dématérialisée, et cette nouvelle façon d'agir en achetant en ligne ou en travaillant en ligne se doit d'être proposée à tous. L'accès matériel au réseau et l'acculturation à celui-ci deviennent ainsi de nouveaux critères témoignant du développement d'un État et de son bon fonctionnement démocratique **(§1)**. Dès lors se dessinent en Europe les contours d'un service universel de l'accès **(§2)**.

[55] Lors de son cours annuel, année 2006-2007.

[56] Voir sur l'usage de ce préfixe, la recommandation de Gabriel de Broglie membre de l'Académie Française, faite en sa qualité de président de la commission générale de terminologie et de néologie en 2002, disponible sur le site du ministère de la culture, culturecommunication.gouv.fr.

§1) L'enjeu démocratique de l'accès au réseau

24. ***Plan***. Dans les pays les plus pauvres les tensions politiques et financières des régimes au pouvoir transparaissent dans les difficultés matérielles d'accès au réseau **(A).** Pour les pays développés et émergents, l'enjeu, alors que l'accès au réseau s'est démocratisé, devient la mise en œuvre d'une bonne « *e-governance* » **(B).**

A] Les problématiques liées à la difficulté d'accès au réseau dans les pays pauvres

25. **Le contrôle stratégique de l'accès au réseau, l'exemple de Cuba.** A Cuba, le contrôle de l'accès au réseau est stratégique. En effet, à l'instar d'autres états communistes, Cuba cherche à intervenir préventivement contre toute forme de dissidence, mais, comme le souligne Frédéric Martel auteur du livre *Smart, enquête sur les internets* [57] *« au lieu d'interdire complètement Internet comme en Corée du Nord ou de construire un immense « intranet » local comme en Chine, Cuba a préféré organisé la pénurie.* »[58]. Les files d'attente devant les rares cybercafés autorisés sont ainsi interminables et les prix prohibitifs. L'importation de téléphones portables, d'ordinateurs et de tablettes est étroitement contrôlée. La mise en œuvre d'un wifi même pour les particuliers, qui sont de fait rares à posséder un accès au réseau, nécessite un permis[59]. Si cette pénurie procède évidemment de la faiblesse économique du pays, elle témoigne néanmoins de la possibilité de contrôle que peut avoir un Etat sur la mise en place des infrastructures d'accès sur son territoire. Le réseau est mondial mais son accès n'est pas uniformisé.

26. **L'enjeu de l'accès à l'éducation numérique, l'exemple de l'Afrique du Sud**. Des disparités apparaissent également non pas au niveau de l'accès physique au réseau, mais eu égard à son usage et à la compréhension de ses fonctionnalités. Le journaliste Frédéric Martel raconte comment menant l'enquête à Kliptown, l'un des bidonvilles les plus déshérités d'Afrique du Sud, il est surpris par l'omniprésence des technologies et de l'internet. L'enjeu est alors celui de la « *digital literacy* » ou alphabétisation digitale, comme le souligne le jeune directeur d'un programme d'éducation au numérique, très populaire dans le bidonville alors qu'il propose également aux enfants de manger gratuitement.

La capacité à savoir utiliser les technologies de l'internet dans un premier temps, puis celle d'apprendre à lire le web, -c'est-à-dire savoir analyser et évaluer les informations que ce nouveau média propose-, est aujourd'hui un facteur de

[57] MARTEL Frédéric, *Smart, enquête sur les internets,* Paris : Stock, 2014, p. 15.
[58] *Ibid* p.10.
[59] Ce permis était nécessaire jusqu'en 2008.

développement économique. A l'heure où une personne sur 7[60] est encore illettrée, il ne s'agit pas d'oublier que l'objectif premier reste d'apprendre à lire à tous ; toutefois, l'acculturation aux réseaux est l'enjeu de demain. Les propos tenus pour promouvoir l'alphabétisation pourraient être repris à l'égard de l'alphabétisation digitale qui peut aussi être envisagée comme un facteur de paix ; elle «*contribue à la paix en aidant chacun à jouir de sa liberté individuelle et à mieux comprendre le monde ainsi qu'à prévenir ou à résoudre les conflits* »[61].

27. **L'enjeu de l'accès à la télémédecine, l'exemple de l'Inde**. Le journaliste Frédéric Martel poursuit son « *enquête sur les internets* » en Inde et interroge le cardiologue de réputation mondiale, le docteur Devi Shetti[62]. Celui-ci lui explique que des centaines de patients font une trentaine d'heures de route pour une simple consultation de dix minutes ; il est dès lors un fervent défenseur de la carte d'identité unique qu'il faudrait relier un jour au dossier médical des patients « *si les données sont bien protégées* ». Il affirme à propos de l'accès aux nouvelles technologies, -et la clarté de son raisonnement mérite de reprendre sa formulation- : « *Et ça prouve aussi la force des technologies : elles peuvent permettre aux pauvres de se rassembler. Les pauvres sont faibles lorsqu'ils sont isolés ; ils sont forts lorsqu'ils sont ensemble. Nous pensons que l'Inde va être le premier pays à dissocier la santé de la richesse. La carte d'identité unique et internet vont nous y aider. L'Inde va prouver au monde que l'on n'a pas besoin d'être un pays riche pour offrir une bonne couverture santé à ses citoyens. Ce n'est plus une question de charité, c'est désormais un droit* »[63].

B] Le développement de l'« e-governance » et de « l'open-data » dans les pays développés et émergents

28. **Les objectifs de l'« *e-governance* »**. L'enjeu de l'administration française est aujourd'hui celui de la mise en œuvre d'une « *e-governance* » effective qui doit permettre à l'usager et à l'administration de gagner du temps et d'économiser de l'argent en ayant accès à des services intégrés et interactifs, qui répondent au mieux à leurs besoins. De nombreuses démarches administratives peuvent se faire en ligne et sont plébiscitées par les citoyens français[64]. Les chantiers de cette « *e-governance* » ne cessent de se développer ; l' « e-santé »

[60] V. les chiffres publiés sur le site de l'« *Institute of statistics* » de l'Unesco à l'occasion de la journée mondiale pour l'alphabétisation le 8 septembre 2013, http://www.uis.unesco.org/literacy/pages/data-release-map-2013.aspx

[61] V. sur le site de l'Unesco, la page consacrée à la journée mondiale pour l'alphabétisation de 2012 ayant pour thème, l'alphabétisation et la paix http://www.unesco.org/new/fr/education/themes/education-building-blocks/literacy/advocacy/international-literacy-day/2012/

[62] MARTEL Frédéric, *Smart, Enquête sur les internets*, Paris : Stock, 2014, chapitre 4 «IT signifie Indian Technologies», p.83-100.

[63] *Ibid.*, p. 92-93.

[64] Voir le baromètre de l'innovation réalisé par BVA pour le Syntec numérique qui indique que 76% des Français souhaitent pouvoir réaliser davantage de démarches administratives sur Internet plutôt que par courrier, par téléphone ou en se

avec la mise en œuvre du Dossier Médical Personnalisé et le développement de la télémédecine, le développement de l'« e-éducation » avec l'apparition pour de nombreuses universités d'environnements numériques de travail qui permettent l'accès à des ressources en ligne, l' « e-justice » avec l'accès aux décisions et aux textes de lois, ainsi qu'aux extraits de casiers judiciaires. La problématique actuelle est celle de « l'open-data » qui consiste « *en une politique d'ouverture et de partage des données publiques* »[65]. Le portail « data.gouv.fr » permet l'accès à plus de 13000 informations publiques gratuites et réutilisables.

29. **L'impact démocratique de l'« open-data »**. Cette logique de la mise à disposition d'informations publiques se constate à l'échelle mondiale alors qu'en juin 2013, le G8 a adopté une charte commune sur le sujet dégageant des principes communs de publicité et d'accès aux données[66]. L'enjeu est à la fois économique et politique. En effet, si l'accès aux données permet l'innovation, il répond également aux exigences d'information des administrés.

L' « e-governance » entendue comme l'informatisation des services administratifs et comme la transparence des données publiques vis-à-vis des usagers est un indicateur de la vitalité des démocraties actuelles qui se veulent de plus en plus interactives et participatives. En France, le décret n°2014-1050 du 14 septembre 2014 institue un « *administrateur général des données* » qui est « *chargé, sans préjudice des missions de l'Institut national de la statistique et des études économiques, de coordonner l'action des administrations en matière d'inventaire, de gouvernance, de production, de circulation et d'exploitation des données par les administrations. Il a également pour mission d'améliorer l'exploitation de ces données et leur circulation, dans le respect de la protection des données personnelles et des secrets protégés par la loi, notamment le secret de la défense nationale* »[67]. La loi pour une République numérique débute ainsi par un titre Ier qui vise *« La circulation des données et du*

---

déplaçant physiquement, BERGE Frédéric, « *E-administration : 75% des français veulent plus de démarches en ligne* », article mis en ligne le 24/01/2014 sur le site 01net.com.

[65] V. la rubrique « *Qui sommes-nous* » sur le site de la mission « Etalab », service du premier ministre chargé de l'ouverture des données publiques et du développement de la plate-forme open-data, etalab.gouv.fr.

[66] Cette charte est disponible en anglais sur le site du « cabinet office » du gouvernement britannique (https://www.gov.uk/government/publications/open-data-charter/g8-open-data-charter-and-technical-annex), la mission Etalab propose un lien vers une version française disponible sur le site Scribd (http://fr.scribd.com/doc/148580461/Charte-du-G8-pour-l-Ouverture-des-Donnees-Publiques-Francais)

[67] Décret 2014-1050 du 1- septembre 2014 instituant un administrateur général des données, JORF n°0215 du 17 septembre 2014, texte n°2.

savoir ». Le chapitre 1er de ce titre est intitulé « *Economie de la donnée* » et sa section première met en œuvre « *l'ouverture de l'accès aux données publiques* »[68].

Les pays émergents mettent en œuvre des plans pour numériser les services de leurs administrations, telle l'Inde qui a lancé son « *nation e-governance plan* » en 2006[69]. A l'été 2014, en Indonésie, au moment de la tenue des élections nationales, c'est une organisation sociale du nom de « Perludem » qui a suppléé au manque d'informations gouvernementales en lançant un site permettant d'avoir accès au profil des candidats, aux données géographiques de l'organisation de l'élection et autres données utiles aux citoyens[70].

§2) L'accès à la structure du réseau et à l'insertion numérique

30. **Promouvoir l'insertion numérique**. A l'été 2013, Google présentait son projet « Loon » en lançant une trentaine de ballons gonflés à l'hélium au dessus de la région de Canterbury en Angleterre. Ces ballons (« *balloons* » en anglais d'où le nom du projet) évoluant dans la stratosphère ont pour but d'apporter une connexion au réseau dans les régions rurales et reculées du globe alors que Google souligne que deux tiers de la population mondiale n'a pas encore accès à internet[71]. L'entreprise américaine se positionne ainsi comme le pourvoyeur d'un nouveau type de réseau mis en œuvre à l'orée de l'espace. Cette initiative qui permet un réel déploiement des connexions mais pose question eu égard à la privatisation de la structure, fait apparaître les véritables enjeux de la mise à disposition d'un accès. Ils ne sont pas techniques mais économiques et politiques.

L'enjeu aujourd'hui n'est plus de combattre la fracture numérique, en référence à la couverture géographique du réseau **(A)** mais bien de promouvoir l'insertion numérique[72], c'est-à-dire le financement de l'accès pour tous et l'acculturation au réseau **(B)**.

---

[68] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF du 8 octobre 2016, Texte 1 sur 96.

[69] Voir les services mis en œuvre sur le portail Web du gouvernement Indien : http://india.gov.in/services/online-services

[70] V. : LUCKMAN Enricko « *Perludem gives developers access to big data about Indonesia's election",* article mis en ligne le 11 mars 2014, sur le site TechinAsia.com.

[71] Voir le site du « project loon » par Google, google.com/loon/

[72] En 2008, dans le cadre de la révision du Paquet télécom, la Commission européenne affirme que : « *L'accès au haut débit n'est pas seulement nécessaire à la compétitivité et à la croissance économique, mais est en train de devenir un élément essentiel du bien-être de la population et de l'insertion numérique* ». V. : Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions sur le deuxième réexamen de la portée du service universel dans les réseaux et services de communications électroniques, conformément à l'article 15 de la directive 2002/22/CE, COM/2008/0572final/, communication non publiée au journal officiel.

A] Le service universel d'accès au réseau mis en œuvre par le « Paquet télécom »

31. **L'obligation de service universel en Europe**. En 2002, dans le cadre du Paquet télécom, est adoptée la directive 2002/22/CE « *concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques* »[73]. La directive définit le service universel comme «l'ensemble minimal des services d'une qualité spécifiée accessible à tous les utilisateurs finals, à un prix abordable compte tenu des conditions nationales spécifiques, sans distorsion de concurrence»[74]. Ainsi les Etats membres ont l'obligation de rendre disponible à tous leurs citoyens l'accès au réseau. Il ne peut y avoir de discriminations liées à la position géographique de l'utilisateur, au montant de ses ressources, ou à la qualité du service fourni.

La France transpose la directive « service universel » en adoptant la loi du 31 décembre 2003[75] qui modifie le Code des Postes et des Communications Electroniques (CPCE) eu égard aux obligations de service public[76]. Un plan de développement numérique pour les années à venir est par la suite élaboré par le gouvernement. Le bilan de « France numérique 2012 » est positif en ce que la fracture numérique a été réduite ; le pourcentage d'individus utilisant internet passant en effet de 26,33% en 2001 à 81,92% en 2013, avec 81,7% de foyers connectés cette même année[77].

Alors que la question n'est plus en France celle de la couverture géographique et de la démocratisation de l'accès, le Conseil National du Numérique dans son rapport « Citoyens d'une société numérique » qui vise « *l'inclusion numérique* », préconise de développer des « *tarifs sociaux ciblés pour l'Internet et le mobile* »[78]. Le Conseil d'Etat rappelle toutefois qu'en l'état de la législation européenne, il n'est pas possible d'inclure de telles prestations dans les obligations de service universel financées par la contribution des opérateurs, et que ces tarifs pourraient alors seulement aujourd'hui être

[73] Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communication électroniques (directive «service universel »), JO L108 du 24.4.2002, p. 51-77.

[74] Directive 2002/22/CE, considérant n°4.

[75] Loi n° 2003-1365 du 31 décembre 2003 relative aux obligations de service public des télécommunications et à France Télécom, JORF du 1er janvier 2004, p.9

[76] CPCE, partie législative, Livre II « *Les communications électroniques* », titre Ier « *Dispositions générales* », chapitre III « *Les obligations de services publics* », articles L35 à L35-7.

[77] Pour une compilation de chiffres utiles (personnes, foyers connectés) et actualisés, voir la rubrique « *data* » du site *thenetmonitor.org.*

[78] Alors qu'il est constaté que « *les dispositifs prépayés finissent par aboutir à des situations dans lesquelles les plus modestes paient plus cher leur minute de communication, leur message, que les autres, plus gros ultisateurs* ! » V. : « Citoyens d'une société numérique, accès, littératie, médiations, pouvoir d'agir : pour une nouvelle politique d'inclusion », Rapport à la Ministre déléguée chargée des petites et moyennes entreprises de l'Innovation et de l'Économie numérique, Octobre 2013, Conseil National du Numérique, p.34. Disponible à cette adresse : http://www.cnnumerique.fr/inclusion/

proposés de manière volontaire par ces derniers[79]. Dans le même sens, la loi pour une République numérique modifie l'article L115-3 du Code de l'action sociale et des familles : le maintien du service d'accès à internet est désormais visé[80]. Une personne ou une famille éprouvant des difficultés particulières, a droit à une aide de la collectivité pour disposer d'un accès au réseau au même titre que l'accès à l'eau, à l'énergie ou aux services téléphoniques. L'accès au réseau ne peut être coupé tant qu'il n'a pas été statué sur une demande d'aide.

Par ailleurs le dynamisme des territoires n'est plus envisagé seulement en terme de pénétration de l'internet dans les foyers mais relève désormais aussi de la mise en œuvre d'une stratégie de développement des usages et services numériques mis à disposition des usagers par les collectivités[81].

B] L'insertion numérique visée par la loi pour une République numérique

32. **L'universalité menacée et les solutions mises en œuvre**. Dans sa contribution à l'ouvrage « *La communication numérique, un droit, des droits* » qui date de 2012, le professeur Bernard Teyssié constatant la fracture générationnelle, économique et géographique dans l'accès à internet dans le monde, affirme qu' « *au principe d'universalité, un coup fatal va être porté* » [82] . Le constat est juste. La mise en œuvre du réseau ne peut se faire uniformément ; l'universalité doit être un souci constant des pouvoirs publics alors qu'elle prend des formes diverses au fil du temps.

Le Conseil National du Numérique a soulevé cet objectif de réduction de la fracture générationnelle et de l'acculturation aux réseaux. Il défend l'idée de l'acquisition d'une « littératie numérique »[83] et prône le développement d'« espaces de médiation », lieux publics de formation et d'accompagnement aux usages du numérique[84]. L'enseignement de l'informatique et de l'usage du réseau, et notamment

---

[79] «Le numérique et les libertés fondamentales », Etude annuelle 2014, Conseil d'Etat, p.92 (édité par la Documentation française et disponible à cette adresse : http://www.ladocumentationfrancaise.fr/rapports-publics/144000541-etude-annuelle-2014-du-conseil-d-etat-le-numerique-et-les-droits-fondamentaux

[80] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, (JORF du 8 octobre 2016, Texte 1 sur 96.), Article 108, dans une section intitulée « *Maintien de la connexion à internet* ».

[81] *Ibid*., v. titre III « L'accès au numérique », chapitre 1er « Numérique et territoires ». Les Schémas Directeurs Territoriaux d'Aménagement Numérique (SDTAN) recensent non plus seulement les infrastructures et les réseaux mais disposent d'un volet relatif à une stratégie de services numériques. L'article L1425-3 du code général des collectivités territoriales est modifié.

[82] TEYSSIE Bernard, « L'homme et la fourmi, variations sur l'empire du numérique », p.55, *in La communication numérique, un droit, des droits,* B.TEYSSIE (*dir*.), Paris : Editions Panthéon-Assas, 2012, 626pp.

[83] « Citoyens d'une société numérique, accès, littératie, médiations, pouvoir d'agir : pour une nouvelle politique d'inclusion », *op. cit*. p. 40. Est présenté le cas d'un individu qui serait confronté à la numérisation de son emploi.

[84] *Ibid.,* p.61. Anciennement appelés des Espaces Publics Numériques, il s'agit de lieux associatifs, médiathèques, foyers de jeunes travailleurs, centres culturels, etc.

l'apprentissage du code[85] font aujourd'hui l'objet d'un plan spécifique de déploiement piloté par le ministère de l'Education nationale de l'enseignement supérieur et de la recherche[86]. Il est à noter également que le la loi pour une République numérique impose aux sites internet des services de l'État d'être accessibles aux personnes handicapées[87]. Les actions de lutte contre « l'illettrisme numérique » sont aussi désormais spécifiquement visées dans les objectifs de la formation professionnelle[88].

Par ailleurs un nouveau plan France-numérique à l'échéance 2020 souligne les enjeux de la protection des données, du « cloud-computing» et de la neutralité du réseau[89]. En effet, il convient d'éduquer les internautes à la protection de leurs données en les informant des choix et des droits qui sont à leur disposition. Par ailleurs, le développement de l'informatique en nuage questionne le financement pour tous d'espaces dématérialisés de stockage[90] et l'accès à un contenu culturel commun[91]. Enfin, garantir l'accès au réseau à chacun n'a de sens que si une fois connecté, l'acheminement du message se fait sans discrimination.

Section II. L'encadrement de l'activité des opérateurs de communications électroniques

33. **L'énigmatique neutralité du réseau.** Dans sa communication « Un statut international pour internet ? », le professeur Mario Bettati indique que l'Iran et la Birmanie contrôlent l'accès au réseau en diminuant temporairement leurs débits ; « *il devient alors très*

[85] V. sur ce point : BARDEAU Frédéric, DANET Nicolas, *Lire écrire compter coder,* Editions FYP (France), 2014. V. également l'initiative de Reshma Saujani, citoyenne américaine, qui a créé l'association « Girls who code » dans le but de permettre aux jeunes filles d'accéder aux métiers de l'informatique, marqués aujourd'hui par leur masculinisation et ce alors que la demande pour ces postes ne cesse d'augmenter, ROSS C., « Reshma Saujani's ambitious plan for Technology », article mis en ligne le 5 novembre 2014 sur le site du *Wall Street Journal*, http://www.wsj.com.

[86] V. sur ce Plan Numérique pour l'Éducation, le site internet dédié et le #EcoleNumerique, http://ecolenumerique.education.gouv.fr/. Ainsi, @Elysée annonce dans un tweet daté du 7 mai 2015 : « "À partir de la rentrée 2016, dès le primaire, les élèves seront initiés au codage" #EcoleNumerique ».

[87] Chapitre III « Accès des publics fragiles au numérique », Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF du 8 octobre 2016, Texte 1 sur 96.

[88] *Ibid*., article 109.

[89] Voir sur le portail Web de l'Economie et des Finances, la page consacrée à France numérique 2020, *http://www.economie.gouv.fr/france-numerique-2020/france-numerique-2020-0*

[90] Il faut souligner en effet les multiples offres de stockage proposées actuellement. Il peut s'agir de services dediés tels *Dropbox* ou *FireDrive* ; les géants du Web proposent également leur coffre-fort numérique comme par exemple l'*iCloud* d'Apple ou le service *Google Drive*. Les problématiques que soulèvent de tels services sont la privatisation du stockage des données et l'accès à ce service alors qu'au delà d'un certain seuil de données, le stockage devient payant.

[91] Le principe de la Licence globale tant décriée il y a un peu plus de dix ans, se réalise aujourd'hui dans le cadre d'initiatives privées telles que les plateformes de musique *Spotify* ou *Deezer* ou les offres d'abonnement à des contenus télévisuels comme *Netflix* ou *Zive*. A la suite de ces services et alors que le schéma de l'accès illimité à un ensemble de contenus en contrepartie d'un abonnement se démocratise, les offres se multiplient ; on peut noter l'initiative de l'INA qui propose un abonnement à 2,99€ par mois, sans contrainte de durée, pour accéder aux archives télévisuelles françaises. Même si certaines des fonctionnalités de ces services peuvent être accessibles gratuitement, leur modèle repose sur l'accès à une utilisation optimale via un abonnement mensuel. L'accès de tous à une offre culturelle commune peut alors être questionné.

difficile de télécharger des photos et des vidéos, voire d'envoyer des courriels »[92]. Cet exemple souligne que l'accès au réseau ne se réduit pas à la possibilité physique d'accéder au terminal et à une boucle du réseau opérationnelle. Il convient, une fois cet accès établi, que la communication soit acheminée de manière telle qu'elle permette une utilisation effective du réseau, c'est-à-dire suivant un débit qui permette un échange de données qui obéit aux choix de l'utilisateur. A défaut, on ne peut parler d'un réel accès au réseau en ce sens qu'il ne permet pas une communication libre.

Sur cet adjectif « libre » qui doit caractériser la communication et sur le terme de « neutralité » il faut toutefois s'entendre**.** Il faut souligner, là encore, que ces termes doivent être dissociés des prétentions libertaires qui les ont vu naître. Comme le souligne Emmanuel Derieux : « *Selon les vœux de certains, le principe dit de « neutralité de l'internet » signifierait la capacité reconnue à chacun, sans aucune forme de restriction ni encore moins de discrimination, d'accéder au réseau mondial de communication en ligne pour y rechercher mais aussi pour y mettre, en toute égalité sinon légalité, tous les messages ou les contenus de son choix, quels qu'en soient la nature et le volume. Formulé par référence au principe de liberté, manifestation d'une conception sans doute plus libertaire que libérale (libéralisme politique ou idéologique et économique), cela peut-il cependant être autre chose que faux-semblant ou tromperie »* [93].

Or la liberté d'accès au réseau ne vise pas les contenus échangés. Elle consiste en la possibilité pour chacun de pouvoir utiliser le réseau selon des conditions qui garantissent l'égalité de traitement de sa connexion, et ce quelque soit les contenus échangés qui font par ailleurs l'objet d'une règlementation. L'enjeu de la neutralité du réseau ne peut être celui du respect de la liberté d'expression et de la mise en ligne de contenus et ne doit pas renvoyer aux problématiques de droits d'auteur et de lutte contre la contrefaçon, ni questionner la légalité de mesures de blocage de certains points d'accès au réseau et de restrictions à la consultation de certains sites.

La neutralité du réseau s'apparente en réalité à une exigence d'égalité pour tous s'agissant de l'accès à ce moyen de communication envisagé comme un service public. Dès lors, ce terme « neutralité » interroge le juriste alors qu'il renvoie à une « abstention » de la part de l'État et de l'opérateur de communications électroniques. Or

[92] BETTATI Mario, « Un statut international pour internet ?», p.97, *in La communication numérique, un droit, des droits*, B.TEYSSIE (*dir*.), Paris : Editions Panthéon-Assas, 2012, 626pp.

[93] DERIEUX E., « Liberté ou surveillance, fondements et éléments du droit de l'internet », *RLDI*-2011, études n°74.

une régulation de cette activité économique doit être mise en œuvre qui permette de garantir *a minima* les objectifs de service public.

34. ***Plan.*** Alors que l'expression de « neutralité du réseau » semble dénommer des réalités diverses qui galvaudent la signification du terme, il convient dans un premier temps de chercher à définir ce que recouvre ce principe qui a trait à la liberté d'accès au réseau et non à la liberté d'expression permise par celui-ci (**§1**). Ce principe de neutralité à l'égard de la mise en œuvre de la connexion fait l'objet aujourd'hui d'une reconnaissance par le droit européen et national qui viennent règlementer les pratiques des opérateurs en vue de la réalisation du service public de l'accès au réseau **(§2**).

§1) La difficile définition d'une obligation de « neutralité » des opérateurs du réseau

35. **La logique de l'acheminement d'un flux de connexion**. Dans son rapport de 2014, intitulé «Le numérique et les droits fondamentaux», le Conseil d'État définit ainsi la neutralité du net qui« *implique que tous les opérateurs d'accès, qu'il s'agisse des fournisseurs d'accès à internet (FAI) en contact avec les utilisateurs finaux ou de ceux assurant l'interconnexion des réseaux, traitent de manière égale tous les flux de données quel que soit leur contenu* ». Il poursuit en rappelant que « *Selon les partisans de la neutralité du net, elle a été déterminante pour favoriser la croissance d'internet et le développement de nouveaux services* : *grâce à elle, chaque innovateur a le même accès à ses clients potentiels. Elle est partie liée avec le droit d'accès à internet et la liberté d'expression : elle permet en effet à chacun d'émettre et de recevoir des contenus dans les mêmes conditions*»[94].

Il faut être réservé sur cette mention de la liberté d'expression qui ne peut être entendue que comme la liberté d'établir et de recevoir des communications et non comme celle de tout mettre en ligne. Il importe ainsi que l'enjeu de la neutralité du réseau soit clairement saisi alors que ce principe renvoie uniquement à la mise en œuvre de l'accès au réseau **(A).** Par ailleurs alors qu'il est souligné que la neutralité de l'internet a été déterminante pour permettre le développement des services du réseau, il convient de s'interroger aujourd'hui sur le régime de cette obligation alors qu'il s'agit désormais de réguler cette nouvelle économie de marché qui est celle des services de l'internet **(B).**

[94] « Etude annuelle 2014 du Conseil d'État-Le numérique et les droits fondamentaux », Paris : La Documentation Française, 2014 (Etude et documents, Conseil d'État), p. 93.

A] L'enjeu de la mise en œuvre de l'accès

36. **La contrainte opérée sur la structure et non sur les contenus échangés**. L'analogie peut être faite avec la problématique, qui apparaît au début du XIXème siècle, eu égard aux pouvoirs des imprimeurs. Ainsi aux *Annales de législation et de jurisprudence,* dans un article intitulé « Du privilège des imprimeurs et de leur devoirs envers le public », Odilon-Barrot s'interroge : « *Les citoyens ont-ils en général le droit de requérir le ministère des imprimeurs ? Ou ce ministère est-il tellement libre et facultatif, que l'imprimeur puisse refuser ses presses sans avoir à en donner d'autre motif que celui de sa propre volonté ? Si les citoyens ont le droit d'obliger les imprimeurs à prêter leur ministère, et si, par suite, ils ont action pour assurer ce droit, devant quelle autorité doit-elle être portée ? La haute importance de ces deux questions est facile à sentir. Il ne s'agit pas seulement de régler les conditions inhérentes à tout privilège, tout monopole, mais de décider si la liberté de la presse, le premier et le plus essentiel de nos droits politiques, viendrait s'évanouir devant le caprice ou l'intérêt des dépositaires privilégiés de l'instrument même de la presse* »[95].

De la même manière la liberté d'accès est conditionnée par la manière dont les fournisseurs d'accès au réseau traitent les connexions de leurs clients. Il n'y a pas de principe de liberté si l'acheminement du message est tributaire de politiques diverses décidées par des opérateurs privés. Il s'agit d'assurer à tous un égal traitement de sa connexion et ce indépendamment de la nature du message, qui fait l'objet d'une règlementation. Etre libre de tout type de connexion sur le réseau, connexion à un réseau P2P, à un serveur de messagerie ou connexion à un site du web quel qu'il soit, ne veut pas dire être libre de tout mettre en ligne sur le réseau.

Une règlementation intervient à cet endroit qui sanctionne une infraction, que celle-ci relève du droit de la presse ou de l'atteinte aux droits d'auteur, ou de tout autre législation spéciale comme le droit de la consommation par exemple. Par ailleurs l'État selon un régime défini est fondé à bloquer certains sites mais ne peut agir sur les flux de connexions en eux-mêmes.

37. **L'abstention des pouvoirs publics s'agissant des flux de connexion.** En effet à l'échelle du gouvernement d'un État, il est évident que tout État dit « de droit » doit s'abstenir de définir une politique de traitement des connexions, comme le choix de limiter les flux P2P ou de décider d'un débit maximal pour chacun ou pour quelques uns ; un choix qui

[95] ODILON-BARROT, « Du privilège des imprimeurs et de leurs obligations envers le public », *Annales de législation et de jurisprudence,* / [Th. Compans, rédacteur principal], n°1 samedi 16 mai 1829, p.5 (Disponible sur Gallica.fr).

serait nécessairement arbitraire en dehors de toute procédure légalement établies visant la privation de l'accès au réseau.

A cet endroit, nous nous opposons fortement à ce qui a pu être envisagé dans le cadre de la lutte contre le téléchargement illégal sur les réseaux P2P alors qu'il était considéré que les FAI devraient « *abandonner l'ancienne rhétorique selon laquelle ils ne seraient que des convoyeurs neutres* (*on sait déjà que ce n'est pas le cas puisque beaucoup gèrent les flux de bande passante de telle manière à réduire le volume occupé pas des système peer-to-peer ou du type Bit Torrent)*» et qu'ils devraient être « *encouragés et (légèrement) contraints-par une loi incitative* » à mettre en œuvre des mécanismes négociés « *qui se rapprocheraient de l'idéal fonctionnel de la riposte graduée* »[96].

Or cette politique de gestion des flux dans le cadre de la lutte contre la contrefaçon porte atteinte à la liberté d'accès au réseau. Quand bien même elle vise la lutte contre un acte illicite, un réseau de P2P et le flux attaché ne réalisent pas la contrefaçon ; il serait arbitraire dès lors d'agir sur le débit d'acheminement de la communication pour limiter l'accès à ces sous-réseaux. Ce procédé est à condamner en ce que, à l'inverse de la mise en œuvre d'une mesure de blocage de sites[97], il ne peut souffrir un régime clair de délimitation et obéir à un impératif de transparence.

38. **Un principe à la charge des opérateurs de communications électroniques**. Le respect du principe de neutralité questionne en réalité la mise en œuvre des connexions par les opérateurs de communications électroniques. Ceux-ci doivent s'abstenir de définir une politique de traitement des connexions qui servirait en dehors de toutes contraintes techniques, leurs seuls intérêts économiques et commerciaux dans une mesure telle que le citoyen serait privé du minima de service public qui à cet endroit lui est dû. Il convient de souligner que l'objet de la « neutralité du réseau » doit se limiter à la mise en œuvre des connexions. Elle vise les opérateurs de communication électroniques qui permettent un accès au réseau et non les services de communication au public en ligne qui mettent en ligne du contenu sur la toile.

En ce sens l'intitulé du rapport du Conseil National du Numérique « *Neutralité des plateformes : Réunir les conditions d'un environnement numérique ouvert et*

[96] V. Dans le cadre du projet de la HADOPI, l'avis n°1481, Enregistré à la Présidence de l'Assemblée Nationale le 18 février 2009 et déposé au nom de la Commission des affaires culturelles, p. 178, disponible sur le site de l'Assemblée Nationale.

[97] V. *infra* : Titre II, Chapitre 1er « Le régime du blocage d'un site : restriction à la liberté de naviguer ».

soutenable »[98] et qui vise les GAFA[99], nous semble maladroit. De fait le terme désormais utilisé est celui de « loyauté » des plateformes, consacré dans une section intitulée « Loyauté des plateformes et informations de consommateurs » de la loi pour une République numérique[100]. Ce principe de loyauté est effectivement dérivé de l'approche américaine de la neutralité du Net[101] et le raisonnement se conçoit : les services du réseau qui opèrent une *« intermédiation »*[102] entre les informations ou les offres disponibles sur la toile et les internautes et ils ne peuvent arbitrairement orienter le classement de celles-ci. Toutefois il faut sémantiquement dissocier la neutralité du réseau de celles des plateformes alors que si leur mise en œuvre peut ressortir des mêmes mécanismes, leurs champs d'application sont différents[103].

B] Le contenu de cette obligation

39. ***Plan.*** Le principe de neutralité renvoie à une exigence de non-discrimination des opérateurs de communications électroniques vis-à-vis des flux transportés **(1),** ce qui ne s'oppose pas à une différenciation des connexions si une régulation transparente et contrôlée est mise en place **(2).**

1) La condamnation de pratiques arbitraires

40. **L'encadrement des pratiques des opérateurs de communications électroniques**. En 2014, le Conseil d'État cite le célèbre article de Tim Wu : « *La neutralité correspond à l'architecture originelle d'internet, qui repose sur le principe du « meilleur effort » (« best effort ») : chaque opérateur fait de son mieux pour assurer la transmission de tous les paquets de données qui transitent sur son réseau, sans garantie de résultat et sans discrimination »*[104].

---

[98] Le rapport en date du 13 juin 2014 est disponible à cette adresse : http://www.cnnumerique.fr/plateformes/ Comme l'indique la page de présentation du rapport sur le site du CNNum : « *Dans son rapport remis le 13 juin 2014 à Arnaud MONTEBOURG, Ministre de l'Economie, du Redressement productif et du Numérique et à Axelle LEMAIRE, Secrétaire d'Etat chargée du numérique, le Conseil national du numérique (CNNum) retient une approche élargie du principe de neutralité : consacrer la neutralité d'Internet et prendre en compte les plateformes numériques, devenues de nouvelles portes d'entrée de la société numérique.* ».

[99] Acronyme renvoyant à *Google*, *Apple*, *Facebook* et *Amazon*.

[100] V. : « Titre II : La protection des droits dans la société numérique », « Chapitre 1er : Environnement ouvert», Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF du 8 octobre 2016, Texte 1 sur 96.

[101] J.ROCHFELD, C.ZOLYNSKI, « La "loyauté" des "plateformes". Quelles plateformes ? Quelle loyauté ? « , *Dalloz IP/IT*, nov. 2016, p.523.

[102] *Ibid.* p. 521.

[103] V. *infra* pour la loyauté des plateformes, Titre II « La liberté de naviguer sur le web », Chapitre 2ème « La règlementation des limitations à la consultation de certains sites et services », Section I : « L'encadrement de l'activité des moteurs de recherche ».

[104] « Etude annuelle 2014 du Conseil d'État-Le numérique et les droits fondamentaux », Paris : La Documentation Française, 2014 (Etude et documents, Conseil d'État), p. 93.

Un article des *Dossiers de la recherche,* intitulé « Menaces sur l'Internet libre et ouvert » [105] explique ainsi de manière très claire ce que recouvre concrètement cette exigence : *« Par exemple un FAI ne doit pas faire circuler les contenus de Dailymotion en priorité même s'il est partenaire du site de vidéo. Et il n'est pas question de brider le concurrent YouTube parce qu'il n'a signé aucun accord. De même un service de téléphonie sur Internet ne doit pas être limité quand un internaute y accède via un téléphone mobile. Et les internautes sont libres d'utiliser à leur gré les réseaux peer-to-peer qui sont tout à fait légaux. Tout cela signifie qu'à l'instar de la poste qui n'a pas le droit d'ouvrir le courrier des usagers, les fournisseurs d'accès n'ont pas à se mêler du type de données qu'ils font transiter. Ni d'interférer sur le contenu du flux. »*[106].

Ainsi la neutralité du réseau, dans une acception qui la restreint et qui donc en permet la délimitation, serait la non-discrimination dans la mise en œuvre de la connexion au réseau en fonction de critères décidés arbitrairement, c'est-à-dire selon un libre choix et qui ne répondrait à aucune nécessité logique[107], ou qui ne serait pas encadré. Le terme discrimination renvoie dans le langage courant à un traitement inégal et défavorable.

41. **La condamnation de l'arbitraire dans le traitement des connexions**. La comparaison avec les services de la poste est pertinente, alors que la poste met en œuvre une communication. La poste ne peut opérer une discrimination dans l'échange des courriers selon des critères fixés *ex-nihilo* en dehors de toute contrainte technique, comme par exemple décider que tous les courriers à destination des prisons seraient mis en attente trois jours avant d'être traités.

Le doyen Gény en ce sens visait déjà la nécessaire impartialité des services de l'Administration des Postes et Télégraphes. Il énonce ainsi : « *Le principe général ainsi établi, devait plus particulièrement, s'adresser d'abord, à l'Administration des Postes et des Télégraphes, qui, instrument nécessaire, en fait, de la transmission des correspondances, et investie d'un monopole de droit important, doit en quelque sorte, à sa propre justification, d'éviter toute indiscrétion, voire même tout semblant de partialité ou de curiosité dans l'exécution de sa mission »* [108].

[105] VIOSSAT Stéphane, « Menaces sur l'Internet libre et ouvert », *Les Dossiers de la Recherche (DLR)* #10-Juin/Juillet 2014, p. 22.

[106] *Ibid.,* p.23.

[107] V. la définition de l'adjectif « arbitraire » sur le site www.larousse.fr/dictionnaires/francais/

[108] GENY François, *Des droits sur les lettres missives, étudiés principalement en vue du système postal français,* Recueil Sirey : Paris, 1911, point 34.

Toutefois, la poste ne peut garantir un même délai de délivrance des plis et un même tarif si les courriers sont de poids ou de destinations différentes[109]. Il ne peut être d'égalité absolue dans l'acheminement des connexions, l'enjeu est alors l'encadrement de ces choix de mise en œuvre par les opérateurs techniques qui peuvent procéder de contraintes techniques ou commerciales.

2) La différenciation possible des tarifs et des offres

42. **Nécessités techniques et différenciation des tarifs**. La discrimination est le fait de critères arbitraires ; ce qui n'empêche pas une différenciation dans le traitement des flux de données. Ainsi la neutralité ne s'oppose pas, à notre sens, à certaines contraintes techniques de gestion du trafic et à la dissociation des offres d'abonnement des opérateurs suivant le débit souhaité pour l'accès à certains services ou contenus. La mise à disposition d'une plus grande quantité de bande passante au détriment des autres utilisateurs doit nécessairement être facturée davantage ; par ailleurs des offres spéciales pourraient être mises en œuvre si un encadrement de ces pratiques était pensé. Le débat autour d'une telle différenciation est encore vif alors pourtant qu'elle ne viserait pas dans un premier temps les particuliers[110].

Une tarification différente de l'utilisation des bandes passantes suivant le débit du service s'opère déjà entre les opérateurs et les services de contenus. Ainsi, aux États-Unis l'opérateur de télécommunications américain *Verizon* était en conflit avec le service de vidéo à la demande *Netflix* qui monopolise le tiers de la bande passante en soirée. Il a obtenu, depuis une décision de janvier 2014 de la cour d'appel des États-Unis (District de Columbia, Washington DC), la possibilité de faire payer plus cher les acteurs du web désireux d'accéder à un débit important[111]. De la même manière en France, l'ARCEP a donné raison fin juillet 2013 au fournisseur d'accès *Free* en conflit depuis de nombreux mois avec la plate-forme de vidéos du groupe *Google, YouTube,* qui refusait de payer plus cher les capacités d'interconnexion alors que son service congestionnait une partie du trafic aux heures de pointes[112].

Tim Wu, professeur de droit américain, le soulignait déjà dans son célèbre article sur la neutralité du réseau : « *les opérateurs poursuivent souvent des buts légitimes tels*

[109] La poste a d'ailleurs annoncé à l'automne 2014 que les tarifs du courrier augmenteraient en moyenne de 7% au 1er janvier 2015, une hausse historique justifiée selon elle par la nécessité de compenser la baisse de l'activité et de financer ses investissements. V. : « La poste : hausse inédite du prix du timbre au 1ER janvier 2015 », article mis en ligne le 1 octobre 2014 sur le site 20minutes.fr

[110] V. : SANYAS Nil, « Orange dément préparer des "offres de débits différenciés"», article mis en ligne le 11/10/2012 sur le site Nextimpaxt.com et REES Marc, « FFT : les "net-goinfres" devront payer pour croquer plus » article mis en ligne le 22/08/2011 sur le site Nextimpaxt.com

[111] V. : LAUGÉE F., « Neutralité du Net : les opérateurs télécoms américains gagnent leur bataille », *Revue Européenne des Médias (REM),* n°29 hiver 2013-2014, p.53.

[112] V. LAUGÉE F., « L'ARCEP, gendarme de la neutralité de l'internet », *REM* n°28, automne 2013, p.14.

que la discrimination par le prix ou de gestion de la bande passante. Le problème consiste en leurs méthodes, comme la censure de certaines applications qui conduit à une distorsion à la fois du marché et de l'évolution des applications. Pour faire court, l'étude de l'évolution récente du marché nous donne de bonnes raisons de penser qu'il faut questionner l'autorégulation –des opérateurs- *dans ce domaine* »[113].

Ainsi, la différenciation de l'acheminement des données n'est pas condamnable en soi, ce qui l'est c'est qu'elle ne soit soumise à aucune règle garantissant une concurrence saine et le maintien d'un service minimum d'accès au réseau. L'autorégulation ne peut être ; une régulation des pratiques doit être mise en œuvre. En ce sens il faut relativiser ce qui a été appelé la « *fin de la neutralité du net aux États-Unis* » en juin 2018.

43. **La fin de la neutralité aux États-Unis**. Dans le cadre de l'administration Obama, en 2015, la neutralité du Net avait été érigée comme un principe fondamental de l'internet alors que l'accès au réseau ne pouvait être à deux vitesses. En décembre 2017[114], ce principe a été remis en cause par une décision de la *Federal Communications commission* (FCC) qui permet désormais aux fournisseurs d'internet de privilégier l'acheminement de certaines données sur d'autres ; on parle alors de voies rapides[115]. La nouveauté est qu'elles vont faire l'objet d'offres spéciales auprès des consommateurs. Par exemple, le fournisseur *AT&T* permet d'accéder selon un débit plus rapide aux contenus de la chaîne *HBO* qui fait partie du même groupe que lui, *TimeWarner*. Ainsi cet opérateur va proposer une offre en ce sens aux internautes désireux d'accéder à ces contenus en priorité[116].

Or cette pratique n'est pas condamnable en soi, même si elle ressort d'un enjeu commercial et concurrentiel. En revanche il est nécessaire d'affirmer les exigences du service public de l'accès pour ensuite venir encadrer ces pratiques. Il faut affirmer que l'accès à l'internet haut débit est un minimum à garantir comme celui de l'accès à l'eau ou à l'électricité ; ce qui ne doit pas empêcher toutefois le développement économique des services de l'internet. Il faut ainsi sortir d'une logique politique du « tout ou rien » qui empêche à la fois toute réflexion autour du contenu d'un service public de l'accès

[113] WU Tim, « Network Neutrality, Broadband Discrimination», *Journal of Telecommunications and High technology law*, 2003, vol. 2, p.143. "*On the whole the evidence suggests that the operators were often pursuing legitimate goals, such as price discrimination and bandwidth management. The problem was the use of methods, like bans on certain forms of applications which are likely to distort market and future of application developpement. In short, the recent historical record gives good reason to question the efficacy of self-regulation in this area."*

[114] " F.C.C. repeals net neutrality rules", article de Cécilia KANG, mis en ligne sur le site du *NewYorkTimes*, le 14 décembre 2017, www.nytimes.com.

[115] « Fin de le neutralité du Net aux Etats-Unis », article d'Etienne COMBIER, mis en ligne sur le site des *Echos*, le 11 juin 2018, www.lesechos.fr

[116] *Ibid.*

mais également toute réflexion s'agissant de la régulation d'une nouvelle économie de marché. L'égalité d'accès au réseau n'équivaut pas à l'uniformité de la prestation qui peut à la marge différer.

§2) L'affirmation d'une exigence minimale de service public

44. **Une exigence minimale de service public**. Il faut souligner que le terme de neutralité apparaît dès 2005 dans le cadre de la refonte du Code des postes et des communications électroniques, refonte qui a pour objet notamment d'opérer la libéralisation partielle du service postal décidée à l'échelle européenne. Ainsi la neutralité dans la transmission du message, pendant de la confidentialité du message, s'inscrit dans la volonté du maintien d'un service public, c'est-à-dire un minima garanti à tout usager face aux offres de ce marché désormais partiellement libéralisé.

De la même manière la neutralité du réseau doit ainsi être envisagée comme recouvrant les exigences du service public de l'accès. L'exigence d'égalité d'accès au réseau notamment a été reconnue par le droit européen et français sous la formulation du « *droit à un internet ouvert* » **(A)**. Ce qui définit un régime visant la gestion du trafic dont le respect est contrôlé par le ministre chargé des communications électroniques et par l'Autorité de Régulation des Communications électroniques et des Postes (ARCEP) **(B).**

A] Le droit à un internet ouvert reconnu par les textes

45. **La « garantie d'accès à un internet ouvert » de la législation européenne.** Dans le cadre de la révision du Paquet télécom, le règlement (UE) 2015/2120 du Parlement européen et du Conseil adopté le 25 novembre 2015 vise à établir *« des mesures relatives à l'accès à un internet ouvert »*[117]. Il modifie la directive 2002/22/CE dite « service universel ». S'il vise clairement à définir et délimiter la neutralité du réseau comme en témoignent les travaux préparatoires à son adoption, ces termes de « neutralité du réseau » ne sont pas repris dans le texte final. L'article 3 de ce règlement s'intitule « Garantir l'accès à un internet ouvert », une formulation adéquate alors que la neutralité consiste bien en l'ouverture de la structure du réseau à toutes les communications indépendamment de leurs contenus et qu'il s'agit bien d'une obligation à la charge des États, obligation qui garantit la liberté d'accès au réseau des citoyens.

[117] Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n°531/2012 concernant l'itinérance sur les réseaux publics de communication mobiles à l'intérieur de l'Union, JOUE du 26/11/2015, L310/1.

Toutefois la construction de l'article 3 semble redondante. En effet, dans un premier temps, cet article, ne vise pas les opérateurs et leurs obligations ; ce sont les utilisateurs finals qui sont d'abord mentionnés. Il est énoncé que ces derniers « *ont le droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet* ». Dans un second temps seulement, il est affirmé que : « *Dans le cadre de la fourniture de services d'accès à l'internet, les fournisseurs de services d'accès à l'internet traitent tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés*. ».

Les deux paragraphes se lisent en creux l'un de l'autre ; c'est le traitement égal des connexions par les fournisseurs de services d'accès qui va permettre aux utilisateurs finals d'accéder à l'ensemble des services du réseau de manière non discriminante. Ainsi l'on regrette cette formulation et cette entame de l'article par « un droit d'accéder » au profit des utilisateurs finals, suivi d'une énumération dont la longueur témoigne de son ineffectivité. La maladresse de la rédaction vient du fait que l'on ne peut énumérer le contenu d'une liberté et que l'on ne peut davantage restreindre sa délimitation en ne visant qu'un seul principe, en l'occurrence ici celui de neutralité, devant la garantir.

46. **Le principe de neutralité reconnu par la loi pour une République numérique**. La loi[118] organise dans un titre II « La protection des droits dans la société numérique » et après avoir visé dans un chapitre 1er l' « *Environnement ouvert* », une première section s'intitule « Neutralité de l'internet ». Toutefois l'article 40 qui vient modifier l'article 33-1 du Code des Postes et des Communications Electroniques opère un simple renvoi au règlement européen. Ainsi au I de cet article, il est désormais prévu que les opérateurs de communications électroniques sont soumis au respect de règles portant sur la neutralité de l'internet telle que visée dans un nouveau « *q)* » qui renvoie à l'accès à un internet ouvert régi par le règlement (UE) 2015/2120.

Ainsi le CPCE est modifié de manière à ce que L'Autorité de Régulation des Communications électroniques et des Postes (ARCEP) puisse contrôler la gestion des

[118] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF du 8 octobre 2016, Texte 1 sur 96.

connexions par les opérateurs de communications électroniques qui doivent permettre à tous leurs utilisateurs l'acheminement de leurs communications dans des conditions optimales.

B] Le contrôle du respect de ce principe par l'ARCEP

47. **La nouvelle mission de l'ARCEP.** Le droit à un internet ouvert interdit le blocage de contenus et de services de manière discriminatoire, notamment pour les opérateurs, à l'égard de services concurrents[119], mais il autorise toutefois une gestion du trafic dite raisonnable pour des « *raisons de sécurité ou pour décongestionner l'accès au réseau »*[120] ; une gestion qui doit donc être transparente et peut être contrôlée. La loi pour une République numérique modifie en ce sens les articles L32-1 et L32-4[121] qui renvoient aux missions du ministre chargé des communications électroniques et de l'ARCEP.

Ainsi au titre de l'article L32-1 II. *5) bis*, la neutralité du réseau est désormais visée. Dans le cadre de leurs attributions respectives, ces deux autorités, dans des conditions objectives et transparentes, doivent prendre des mesures raisonnables et proportionnées en vue d'atteindre cet objectif.

Dès lors, pour ce faire, en application de l'article L32-4 I. 2°, le ministre et l'ARCEP peuvent recueillir auprès des personnes fournissant des services de communication au public en ligne les informations ou documents concernant non seulement les conditions techniques et tarifaires d'acheminement de leur trafic, mais également les règles de gestion qui leur sont appliquées par les opérateurs pour vérifier que la neutralité de la transmission de leurs services est bien assurée.

48. **Les outils à disposition de l'ARCEP.** L'article L36-7 est également modifié en 2016[122]. Il est affirmé que l'une des missions de l'ARCEP consiste à contrôler que les opérateurs respectent bien cette exigence de neutralité prévue par le règlement (UE) 2015/2120. L'article L36-8 II *5°* énonce ainsi dans sa nouvelle version[123] que l'Autorité de régulation des communications électroniques et des postes peut être saisie des différends portant sur : « *Les conditions réciproques techniques et tarifaires d'acheminement du trafic, y*

[119] Ce qui à l'inverse des États-Unis, ne permet pas actuellement en France à un opérateur de privilégier le débit s'agissant de ses offres propres de contenus.

[120] V. LAUGÉE F., « L'ARCEP, gendarme de la neutralité de l'internet », *REM* n°28, automne 2013, p.14.

[121] Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF du 8 octobre 2016, Texte 1 sur 96, article 40.

[122] *Ibid.*

[123] *Ibid.*

compris de gestion, entre un opérateur et une entreprise fournissant des services de communication au public en ligne, en vue notamment d'assurer le respect de la neutralité de l'internet mentionnée au q du I de l'article L. 33-1 du présent code ».

Enfin l'article L36-11 est modifié également[124] de manière à ce que le pouvoir de sanction de l'autorité administrative indépendante puisse être mis en œuvre en cas de manquement aux exigences de du règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert.

[124] *Ibid.*

Conclusion Chapitre 1er

49. **La logique d'une liberté publique**. Dans son article « *Le droit d'accès à Internet, nouveau droit fondamental* », la professeure Laure Marino introduit son propos en indiquant que « *l'on peut se réjouir de cette création* [par la décision du Conseil constitutionnel du 12 juin 2009] *d'un nouveau droit-liberté : le droit d'accès à Internet* »[125]. Elle argumente toutefois que celui-ci n'implique pas forcément la reconnaissance d'un droit-créance, fondement d'une prestation pour l'Etat. Elle conclut alors : « *Autrement dit, il ne nous paraît pas judicieux de reconnaître en plus du droit d'accès consacré par le Conseil, un véritable droit à l'accès (comme certains amendements législatifs le proposent)* »[126].

Cette prudence quant à la formulation d'un « droit à » est compréhensible en ce qu'elle procède de fait d'une méfiance quant à la subjectivisation des droits fondamentaux. Il convient de veiller toutefois à ce que l'on ne tombe pas dans le travers inverse qui ne reconnaîtrait pas à un droit à l'objet défini, son caractère fondamental. La distinction « *droit d'accès* » et « *droit à l'accès* » n'est pas opérante ici. L'usage par le professeur Marino de l'expression « droit-liberté » est révélateur de la logique du besoin pour tous d'un accès au réseau qui est celle d'une liberté publique.

50. **La consécration d'un service public d'accès à internet**. Laure Marino ose affirmer que « *C'est au fond-disons le mot- un service public de l'accès à internet qu'il faudrait mettre en place, comme il existe un service public de l'éducation* »[127]. Elle dissocie alors, à juste titre, pour appuyer sa position, ce service public d'un « *droit à l'accès à internet*» qui serait un « *droit-créance, fondement d'une prestation* ».

En effet, la mise en œuvre d'un service public d'accès à l'internet consiste en une série d'obligations pour l'Etat qui ne fondent pas un droit à une prestation générale qui n'aurait pas d'objet défini. Autrement dit le citoyen est seulement fondé à réclamer la mise en œuvre du service public qui s'inscrit dans la limite de la satisfaction de l'intérêt général. Les limites de la prestation matérielle de ce service public viennent d'être dessinées. L'accès en tous les points du territoire doit être possible selon un débit minimum garanti. Cet accès n'a de sens que s'il est mis à disposition des citoyens des

[125] MARINO Laure, « Le droit d'accès à Internet, nouveau droit fondamental », *D.*2009 n°30, Point de vue, p.2045.
[126] *Ibid*., p. 2046
[127] *Ibid*.

outils pour s'acculturer au réseau et exploiter l'ensemble de ses possibilités[128]. Une fois la connexion établie, elle ne doit pas faire l'objet de discriminations créées *ex nihilo*[129].

Il apparaît que la satisfaction de cet intérêt général se réalise en Europe et en France, et ce à l'inverse d'autres Etats[130], alors qu'elle répond à des mécanismes éprouvés qui permettent la conciliation des mécanismes d'une économie de marché avec la défense de l'intérêt général. La mise en œuvre d'un véritable service public ne peut toutefois se réaliser sans l'impulsion d'une véritable politique publique.

51. **La cohésion des principes à mettre en œuvre**. Ce besoin d'une politique de l'accès au réseau n'est pas nouveau. Dans leur rapport sur l'informatisation de la société datant de 1977, MM. Nora et Minc s'exprimaient déjà en ces termes : « *La politique des réseaux décidera si la télématique reste l'activité de quelques puissantes féodalités, ou si elle se diffuse démocratiquement. […] Selon le degré d'ambition assigné à la politique de normalisation, elles*-les télécommunications- *peuvent « encadrer » l'informatique […] Cette politique suppose un projet à long terme de la part de l'Etat, de vigoureuses capacités d'arbitrage, mais aussi des organismes d'exécution dynamiques, souples et attentifs au marché. Ces préalables ne sont aujourd'hui pas satisfaits. […] Celles-ci peuvent aller jusqu'à la séparation des postes et télécommunications, et la création d'un ministère des Communications coordonnant les actions à long terme de toutes les parties prenantes* ».[131]

La récente loi pour une République numérique a le mérite, de par son titre déjà, d'attirer l'attention sur le fondement démocratique de l'encadrement du réseau. Par ailleurs elle met en œuvre des dispositions dessinant le service public de l'accès. Les avancées gouvernementales visant une France Numérique et une École Numérique sont notables. Ces initiatives trouveraient toutefois leur cohésion dans la reconnaissance d'une nouvelle liberté fondamentale. En effet, le taux de pénétration d'internet dans les foyers français et la facilité déconcertante qu'ont les jeunes générations à appréhender ce nouveau moyen de communication, d'expression et d'action, témoignent de ce qu'est

[128] V. sur des propositions concrètes de nouveaux services à disposition des usagers, *supra* Section I, §2 :« L'accès à la structure du réseau et à l'insertion numérique»

[129] V. sur la mise en œuvre déjà effective de ces limites, *supra* Section II : « L'encadrement de l'activité des opérateurs de communications électroniques ».

[130] V. sur ce point, l'analyse de Frédéric Martel sur la pénétration des téléphones mobiles et de l'accès à Internet en Amérique latine. Au Mexique, l'abus de position dominante dû au monopole de l'entreprise de télécommunications de Carlos Slim rend l'accès à Internet dans ce pays le plus lent et le plus cher du monde. Le Brésil quant à lui souffre encore d'une discrimination dans l'accès au réseau selon les classes sociales alors qu'une grande partie de la population ne parle pas anglais et s'intéresse surtout à des contenus locaux. MARTEL Frédéric, *Smart, Enquête sur les internets,* Paris : Stock, 2014, chapitre 3 « Mobile », p.69-81.

[131] V. NORA S., MINC A, *L'informatisation de la société, Rapport à M. le Président de la République* (remis le 20 janvier 1978), Paris : Seuil, 1978 (coll. Points), Introduction du chapitre 1 de la 2ème partie « Le pôle des télécommunications », p. 75-76.

l’accès au réseau : une liberté. L’individu s’en empare sans qu’il y ait besoin de la promouvoir. En revanche, l’État doit formellement la reconnaître pour la garantir efficacement.

Chapitre 2ème. La reconnaissance du caractère fondamental de ce nouveau principe

52. **La liberté d'accès au réseau et non le droit à un « Internet libre »**. La revendication d'une liberté d'accès au réseau doit être dissociée de toute prétention libertaire quant à l'usage du réseau et de ses applications. Il ne s'agit pas d'affirmer que eu égard à l'esprit qui l'a fondé, l'internet ne doit pas faire l'objet d'immixtions étatiques alors que sa nature même permet une autorégulation efficace. Le juriste ne peut être que circonspect face à l'adjectif « neutre ». Il n'est pas question ici de la liberté sur le réseau mais de la liberté d'accès à celui-ci. Il ne s'agit pas de protéger la liberté d'utilisation du réseau ; il faut garantir l'accès au réseau. La construction est inverse : l'État doit mettre en œuvre une nouvelle liberté publique.

Il semble important de préciser dès à présent cette différence de position alors que la problématique des conditions de la coupure d'accès au réseau et donc de la nature du droit d'accès au réseau sont apparues dans le contexte sensible de la lutte contre le téléchargement illégal. Deux positions s'opposaient alors. Le droit d'accès était défendu par les tenants d'un internet dit « neutre » ou « libre » pour qui le réseau ne pouvait souffrir l'intervention étatique ; la neutralité selon eux ne renvoyait pas seulement à l'égal traitement de la connexion pour tous mais également à une neutralité d'actions sur les contenus qui interdisait alors tout filtrage. Le droit d'accès à l'internet se diluait ainsi dans un droit à l'internet libre tant au niveau de son fonctionnement technique que de ses contenus. Or si c'est à bon droit que ces défenseurs de l'autorégulation arguaient du fondement démocratique de l'accès à internet, celui-ci ne peut toutefois rendre tous les usages licites et ne s'oppose pas à tout blocage de sites ou privation d'accès[132]. Inversement, les défenseurs du droit d'auteur et des droits voisins, pour leur part, semblaient réduire l'accès à internet à son seul aspect de nouveau mode d'expression qui devait être d'autant limité que l'atteinte au droit d'auteur était importante.

Cette opposition frontale alors qu'il semblait qu'on ne pouvait défendre le droit d'accès sans être taxé de méconnaître le droit d'auteur ou inversement, a desservi le

[132] V. sur cette « illusion libertaire » et le « culte d'internet » : SCHMIDT-SZALEWSKI J., « L'internet ou l'illusion libertaire », *in Mélanges Simler,* Paris : Dalloz, Litec LexisNexis, 2006, p.803.

droit d'accès qui s'il est strictement défini comme la mise en œuvre de l'accès au réseau n'est pas une revendication libertaire mais s'inscrit au contraire dans notre système éprouvé de libertés publiques. La liberté d'accès au réseau doit être reconnue comme une liberté de premier ordre permettant l'exercice de toutes les autres.

53. ***Plan.*** Il est ainsi proposé de consacrer le rattachement du principe de la liberté d'accès à la liberté individuelle garantie par l'article 66 de la Constitution **(Section I.),** ce qui permet de définir clairement les conditions de la privation d'accès au réseau **(Section II).**

Section I. Le possible rattachement à la liberté individuelle

54. **Le contexte de la création d'une sanction consistant en la coupure d'accès au réseau.** Au printemps 2009, une procédure d'adoption difficile aboutit la loi « *favorisant la diffusion et la protection de la création sur Internet* »[133]. Cette loi créé la « *Haute Autorité pour la Diffusion des œuvres et la Protection des droits sur Internet* » dite « HADOPI » qui a pour fonction notamment de mettre en œuvre la riposte graduée. Le constat d'un téléchargement d'une œuvre protégée conduit à l'envoi d'une première recommandation par message électronique, puis d'une deuxième assortie de l'envoi d'une lettre remise contre signature. Dans la version de la loi, avant qu'elle soit soumise au Conseil constitutionnel, la troisième étape consistait en la décision prise par l'HADOPI de suspendre, pour une durée de deux mois à un an, l'accès de l'abonné sanctionné alors non pas pour contrefaçon mais pour défaut de surveillance de son accès[134].

Le Conseil constitutionnel saisi par soixante députés et soixante sénateurs censure la riposte graduée sur le fondement de la liberté de communication et d'expression de l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen (DDHC). La coupure d'accès eu égard à l'importance de cette liberté dans une société démocratique ne peut pas être mise en œuvre par une autorité administrative en dehors de toute procédure judiciaire[135]. Cette annexion à la liberté de communication et d'expression est une position qui à juste titre ne satisfait pas les défenseurs du droit d'auteur **(§1)**. Elle ne devrait pas davantage satisfaire les tenants de la reconnaissance

[133] V. : Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n°0135 du 13 juin 2009, p.9666, texte n°2 V. également : le dossier législatif de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, disponible sur le site de l'Assemblée Nationale, assemblée-nationale.fr.

[134] La définition de cette obligation se devait d'être distincte du délit de contrefaçon eu égard au principe de légalité des délits et des peines.

[135] *Cons. Const., déc.* n°2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*.

d'un droit à l'accès alors que le rattachement qui apparaît opportun est celui de la liberté individuelle **(§2)**

§1) Le rattachement maladroit de la liberté d'accès à la liberté de communication

55. **Le rattachement de la liberté d'accès à l'article 11 de la DDHC**. Dans le considérant 12 de sa décision visant la « *Loi favorisant la diffusion et la protection de la création* sur internet », le Conseil constitutionnel rappelle le contenu de l'article 11 de la DDHC qui promeut la « *libre communication des pensées et des opinions* » et affirme : « *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 des opinions, ce droit implique la liberté d'accéder à ces services* ». Le Conseil constitutionnel rappelle alors de manière « presque "classique" »[136] : « *la liberté d'expression et de communication est d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés ; que les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi* »[137].

Cette forte connotation démocratique de la liberté d'expression en fait la liberté adéquate pour y annexer l'accès à internet, dont l'importance est pressentie sans toutefois que la valeur d'un droit fondamental qui y serait attaché soit dégagée. Toutefois, ce rattachement restreint le raisonnement à un seul aspect du réseau : celui de l'expression en ligne **(A)** et ne permet pas de considérer un régime cohérent de la coupure d'accès au réseau **(B).**

A] Le champ structurellement limité du « droit de la communication »

56. **Le réseau, réduit à son application web et à la diffusion d'informations**. Le constitutionnaliste Michel Verpeaux dans son étude de la décision souligne que le Conseil constitutionnel aurait pu citer la possibilité d'usage professionnel d'internet, qui renvoie à la

---

[136] VERPEAUX Michel, « La liberté de communication avant tout, la censure de la loi Hadopi 1par le Conseil constitutionnel », *JCP*, 2009, n°39 du 21 septembre, étude 274, p.49

[137] Un raisonnement en effet adopté pour la première fois dans une décision portant sur la loi « *visant à limiter la concentration et à assurer la transparence financière et le pluralisme des entreprises de presse* ». V. : *Cons. Const., déc.* n°84-181 DC des 10 et 11 octobre 1984.

Ce considérant n'est pas sans rappeler celui de la Cour Européenne des Droits de l'Homme dans l'arrêt *Handyside* du 7 décembre 1976 (cons. 49) : « *Son rôle de surveillance commande à la Cour de prêter une extrême attention aux principes propres à une "société démocratique". La liberté d'expression constitue l'un des fondements essentiels de pareille société, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun […] D'un autre côté, quiconque exerce sa liberté d'expression assume "des devoirs et des responsabilités" dont l'étendue dépend de sa situation et du procédé technique utilisé.* », CEDH, 7 décembre 197, *Handyside c. Royaume-Uni.*

liberté du commerce et de l'industrie[138]. Le réseau en effet ne se réduit pas au web et à la possibilité pour chacun de mettre du contenu en ligne.

Toutefois le commentaire de la décision dans « *Les cahiers du Conseil constitutionnel* » précise pour justifier ce choix que *« Internet peut également constituer un outil professionnel permettant l'exercice de la liberté du commerce et de l'industrie, mais, fondamentalement, au-delà des usages qu'il peut être fait, il est d'abord, un moyen de communication* »[139] ; la communication étant entendue ici dans son acception juridique, qui ne peut se départir d'une volonté de rendre publique une information[140]. De fait, comme le soulignait déjà le Doyen Favoreu, *« de la liberté de communication, on ne peut que rapprocher la "liberté d'expression"* »[141].

57. **La dimension active de la liberté de communication**. Le commentaire aux *Cahiers du Conseil constitutionnel* rappelle ainsi que la liberté de communication et d'expression n'est pas ici seulement envisagée dans sa dimension passive pour le citoyen dès lors « *récepteur d'informations* »[142], mais bien aussi dans sa dimension active alors qu'internet permet de nouvelles formes d'expression accessibles à chacun, tels : « *le courrier électronique, le Web 2.0, les blogs….* ». Ainsi il est affirmé qu'« *il y avait d'autant moins de raison de ne pas faire bénéficier ces moyens d'expression de la garantie de l'article 11 de la Déclaration de 1789 que sa lecture littérale invite d'abord à une protection de la dimension « active » de ce droit de « parler, écrire, imprimer, librement* »[143].

Or quand bien même le Conseil insiste ici sur la dimension active d'une telle communication désormais à la portée de tout quidam, elle ne permet pas de recouvrir le véritable enjeu du réseau qui permet la communication entendue de manière générale comme la mise en relation des individus et les activités que cela permet. Au contraire une maladresse structurelle apparaît alors que le rattachement de la liberté d'accès au réseau à la liberté d'expression induit un rapport de proportionnalité déjà éprouvé avec un droit fondamental de même valeur, le droit de propriété des articles 2 et 17 de la

[138] VERPEAUX Michel, « La liberté de communication avant tout, la censure de la loi Hadopi 1par le conseil constitutionnel », *JCP*, 2009, n°39 du 21 septembre, étude 274, p.46.

[139] *Cah. Cons. Const.* 2009 n°27, p.104.

[140] Ainsi le *Vocabulaire Cornu,* définit la communication comme le « *fait de porter un évènement ou élément d'information à la connaissance d'une personne déterminée (adversaire, organe de contrôle) d'un groupe d'intéressés ou du public* ». CORNU Gérard (*dir.*), Association Henri Capitant, *Vocabulaire juridique.* 10ème éd. Paris : P.U.F., 2014 (Quadrige).

[141] V. : FAVOREU Louis, « Le droit constitutionnel jurisprudentiel en 1981-1982 », *RD publ.* 1986, p.387.

[142] V. : *Cons. Const., déc.* n°84-181 DC des 10 et 11 octobre 1984, considérant 38 : « *en définitive, l'objectif à réaliser est que les lecteurs, qui sont au nombre des destinataires essentiels de la liberté proclamée par l'article 11 de la Déclaration de 1789, soient à même d'exercer leur libre choix* ».

[143] *Cah. Cons. Const.* 2009 n°27, p.104.

DDHC qui va s'avérer impossible dès lors que la sanction du déséquilibre ne peut être la coupure d'accès au réseau.

B] Le régime incohérent de la coupure d'accès au réseau

58. **L'impossible conciliation de la liberté d'expression et du droit de propriété**. Le droit de propriété fait lui aussi l'objet, à l'instar de la liberté de communication et d'expression, d'une approche extensive qui vise les droits d'auteurs et les droits voisins[144]. Une conciliation doit avoir lieu entre la protection de la liberté d'expression et la protection du droit d'auteur ; autrement dit, l'atteinte portée à la liberté d'expression doit être proportionnelle à celle portée au droit d'auteur. Or, ici, la maladroite annexion du droit d'accès à la liberté d'expression tend à faire penser que ce jugement de valeur n'aura plus jamais lieu dès lors que le réseau sera utilisé.

Plusieurs commentateurs de la décision de 2009 soulignent leur malaise : « *La propriété intellectuelle passe à la trappe, le Conseil constitutionnel ne se livre jamais à l'arbitrage des droits qu'il annonce* »[145], ou encore « *Compte tenu de l'attention dont fait l'objet cette liberté, il parait difficile de soutenir qu'il n'y a pas de hiérarchie au sein du bloc de constitutionnalité, ou au moins que le conseil n'a pas de préférence* »[146]. Si Michel Verpeaux souligne que la conciliation ne veut pas dire que le Conseil peut renvoyer le droit d'auteur et la liberté de communication dos-à-dos mais implique de trancher dans un sens ou un autre[147], la justification du choix de la liberté de communication eu égard à son importance démocratique n'est pas satisfaisante.

En effet, le recours à la liberté d'expression qui fait écran entre l'accès et l'atteinte au droit d'auteur envisagée ici à savoir le téléchargement illégal d'œuvres protégées, déplace le débat sur le terrain du contenu et de la mise en ligne. Dès lors, il est légitime que les défenseurs du droit d'auteur s'indignent. Ainsi alors qu'il n'est jamais dit que la coupure d'accès est une sanction trop forte eu égard à l'infraction constatée mais que l'importance du droit d'expression dans une société démocratique justifie le maintien de l'accès en dehors de toute procédure judiciaire, ils sont fondés à s'interroger sur les limites non pas de l'accès mais bien de l'usage du réseau.

59. **La nécessité de considérer le réseau comme un nouvel état de fait.** L'annexion maladroite à la liberté d'expression conduit à dessiner en creux un droit à l'expression sur le

[144] V : *Cons. Const., Déc.* n°2009-580 DC, considérant 13.

[145] BRUGUIERE Jean-Michel, « Loi "sur la protection de la création sur internet" : mais à quoi joue le Conseil constitutionnel ? », *D.* 2009, n°26, point de vue, p.1771.

[146] DE LAMY Bertrand, « Hadopi 1 : Précisions du Conseil constitutionnel sur le pouvoir de punir », *RSC.* 2010.209.

[147] VERPEAUX Michel, *ibid*., p.49.

réseau qui ne pourrait souffrir de censure. Le rapport de proportionnalité est biaisé par la référence à l'usage spécifié du réseau. La décision donne cette impression que non seulement l'accès physique au réseau ne peut être coupé mais qu'également l'accès à l'expression en ligne ne peut être restreint. Elle renvoie donc maladroitement à ce qu'elle devrait combattre, le sentiment qu'internet, dans ses contenus, puisse être neutre, autrement dit un espace de non-droit.

Ce sentiment d'une expression en ligne intouchable est renforcé alors que la justification de l'interdiction faite à l'autorité administrative qu'est l'HADOPI de restreindre la liberté d'expression en coupant l'accès n'obéit pas à la logique traditionnelle du Conseil constitutionnel qui, d'une part permet la régulation des moyens de communication[148] et qui d'autre part, permet la mise en œuvre de sanctions par une autorité administrative dès lors que celle-ci n'est pas privative de liberté physique et que son prononcé est entouré de garanties juridictionnelles[149].

De fait, il convient de supprimer la référence à la liberté d'expression qui empêche la considération de l'enjeu de l'accès à internet qui est celui d'être libre d'accéder à toutes les possibilités d'action qu'offre ce nouvel environnement. La coupure d'accès est une peine privative de liberté ; une liberté qui n'est certes pas celle du corps physique mais qui peut toutefois s'appréhender matériellement alors que l'accès au réseau permet l'interaction avec le monde réel.

§2) L'interprétation créatrice possible de l'article 66 de la Constitution

60. **L'interprétation créatrice de l'article 66 de la Constitution.** Le commentaire de la décision du Conseil constitutionnel aux Cahiers, précise la portée de celle-ci : « *La reconnaissance d'une telle liberté ne revient pas à affirmer, comme le soutenaient les requérants, que l'accès à internet est un droit fondamental. Affirmer la liberté d'accéder à internet ne revient pas à garantir à chacun un droit de caractère général et absolu d'y être connecté* »[150]. Ce souci de réaffirmer qu'un droit ne peut être général et absolu, témoigne à cet endroit encore de la peur d'affirmer un nouveau principe fondamental sans en avoir délimité les contours.

[148] V. : DERIEUX Emmanuel, « Les principes du droit de la communication dans la jurisprudence du Conseil constitutionnel, de la liberté de communication au droit à la communication », *Légipresse*, n°141, mai 1997, II-50.

[149] Selon une jurisprudence constante, v. : *Cons. Const., déc.* n°89-260 DC du 28 juillet 1989, cons. 6 (décision relative aux pouvoirs de sanction de la COB) et *déc.* n°97-389 DC du 22 avril 1997, cons. 3.

[150] *Cah. Cons. Const.* 2009 n°27, p.104.

Or le Conseil constitutionnel pourrait tout à fait par une interprétation créatrice de l'article 66 considérer que la possibilité d'accéder au réseau et donc d'agir dans ce nouvel espace dématérialisé qu'il crée, s'apparente à la sûreté personnelle de l'individu dans le monde physique. L'article 66 énonce en effet que : ««*Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi. »*[151].

Le caractère fondamental de la liberté d'accès serait alors posé **(A),** ce qui en permettrait une délimitation claire à travers le régime applicable à la privation de liberté physique de l'individu **(B).**

A] La consécration du caractère fondamental de la liberté d'accès au réseau

61. **Consacrer la liberté fondamentale de l'accès au réseau.** Il a été constaté à travers divers exemples que l'accès au réseau est en lui-même aujourd'hui une condition de la démocratie. Son caractère fondamental peut et doit être fondé sur son lien indissociable avec le régime démocratique. Seuls les régimes dictatoriaux limitent aujourd'hui l'accès physique au réseau, soit en pratiquant un régime d'autorisation, soit en réduisant le débit de la connexion. Ainsi, ils opèrent une mainmise non seulement sur les informations accessibles à leurs citoyens mais également sur leur capacité d'action et donc sur la possibilité qu'ils auraient de vivre et de s'organiser en dehors des contraintes autoritairement établies.

Le réseau permet de nouvelles modalités d'exercice de l'ensemble des libertés et droits séculairement reconnus : liberté d'opinion et de pensée eu égard au pluralisme du contenu des sites web, liberté de commerce et de l'industrie eu égard à la diversité de ses applications, liberté de communiquer et de s'exprimer eu égard à son interactivité. L'individu dans une société démocratique ne peut être privé du nouvel usage de l'ensemble de ses libertés par le seul vouloir de l'autorité étatique ; l'individu ne peut être privé arbitrairement de l'accès au réseau.

62. **La délimitation de la liberté d'accès au réseau**. Cette affirmation ne fonde pas un « droit à l'accès » général, et n'équivaut évidemment pas à l'affirmation d'une liberté d'expression sans limites. La sûreté physique de l'individu et sa liberté d'accès au réseau sont conditionnées par le respect des règles établies pour garantir, dans une acception plus large, la sûreté de la société dans laquelle il vit. Le pendant de la liberté est la responsabilité.

[151] Article 66 de la Constitution du 4 octobre 1958, Titre VIII « De l'autorité judiciaire».

Ainsi l'individu est libre d'accéder au réseau tant qu'il ne méconnaît pas les règles qui fondent la vie en société dans une mesure telle qu'il serait légitime de le sanctionner en le privant de toute capacité d'action eu égard à cette société. Ce rapport entre l'acte commis et une privation de toute liberté d'action est du ressort du législateur. De plus, eu égard à son importance, cette sanction ne peut être mise en œuvre que par l'autorité judiciaire.

B] Le régime de cette liberté

63. **Le juge de la privation de liberté**. Le Conseil constitutionnel dans sa décision du 10 juin 2009 ne censure pas la possibilité de couper l'accès au réseau, mais affirme dans son considérant 16 que « *eu égard à la nature de la liberté garantie par l'article 11 de la déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins* »[152].

Cette affirmation déstabilise les commentateurs[153] alors qu'elle va à l'encontre d'une jurisprudence constante du Conseil constitutionnel qui d'ordinaire affirme que le principe de séparation des pouvoirs ne s'oppose pas à ce qu'une autorité administrative prononce une sanction dès lors que celle-ci n'est pas privative de liberté et que le principe de légalité des délits et des peines ainsi que les droits de la défense, sont respectés[154]. Or ici, il est affirmé que la HADOPI n'aurait pu prononcer une telle sanction « *quelles que soit les garanties encadrant le prononcé des sanctions* ». Comme le souligne le professeur de Lamy : « *Si en l'occurrence seule la nature de la peine-en l'occurrence une peine privative de liberté-empêchait son prononcé par les autorités administratives, il faut désormais considérer que le pouvoir de sanction desdites autorités peut être éclipsé par la nature de la liberté qu'il s'agit d'encadrer »*[155]. Ce nouveau critère laisse perplexe alors que la liberté de communication et d'expression de

[152] Conseil constitutionnel, décision n°2009-580DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, JORF du 13 juin 2009, p.9675

[153] V. : BRUGUIERE Jean-Michel, « Loi « sur la protection de la création sur internet » : mais à quoi joue le Conseil constitutionnel ? », *D.* 2009, n°26, p. 1770. LAMY de, Bertrand, « HADOPI 1 : Précisions du Conseil Constitutionnel sur le pouvoir de punir », *RSC* 2010, n°209.

[154] Décision 89-260 DC du 28 juillet 1989, loi relative à la transparence et à la sécurité du marché financier (sur les pouvoirs de la COB), et Décision 97-389 DC du 22 avril 1997, loi portant diverses dispositions relatives à l'immigration. V. : CAPELLO Aurélie, « Retour sur la jurisprudence du Conseil constitutionnel relative aux sanctions administratives », *RSC* 2014, n°15. V. également pour une application récente : la décision 2013-331 QPC du 5 juillet 2013, Société Numéricâble SAS et autre [Pouvoir de sanction de l'Autorité de régulation des communications électroniques et des postes] par laquelle le Conseil Constitutionnel censure des dispositions qui *« n'assurent pas la séparation, au sein de l'Autorité, entre, d'une part, les fonctions de poursuite et d'instruction des éventuels manquements et, d'autre part, les fonctions de jugement des mêmes manquements, méconnaissant le principe d'impartialité* ».

[155] LAMY de, Bertrand, *op. cit.*

l'article 11 ne peut avoir dans la hiérarchie des normes une valeur plus importante que les autres libertés consacrées par la constitution.

En revanche, l'affirmation des sages de la rue Montpensier se conçoit dès lors qu'il apparaît que la privation d'accès à internet peut s'apparenter à une privation de l'ensemble des libertés de l'individu s'exerçant grâce au réseau, privation qui ne peut être décidée que par le juge judiciaire et obéir à des conditions strictes.

Section II. Les conditions de la privation d'accès au réseau

64. **La pertinence du régime garantissant la sûreté corporelle de l'individu**. Couper l'accès au réseau d'un individu peut renvoyer à la sûreté au sens strict : on ne peut arbitrairement décider de priver l'individu de l'accès au réseau qui permet l'exercice de toutes les libertés qui lui sont constitutionnellement reconnues.

L'interdiction de l'accès à internet dans les prisons françaises vient appuyer cette position : la privation de liberté physique conduit nécessairement à la restriction de la liberté d'accès au réseau **(§1).** Dès lors les cas de privation de l'accès à internet en dehors de toute détention physique doivent être strictement définis et mis en œuvre **(§2)**

§1) Les restrictions à la liberté d'accès au réseau constitutives à la mise en détention

65. **L'interdiction de l'internet en prison**. Dans les faits, actuellement, l'accès au réseau n'est pas mis en œuvre dans les prisons françaises et aucun régime d'utilisation de cet outil de communication à l'instar de celui de la correspondance des détenus ou de leur accès au téléphone n'a été établi[156]. Le contrôleur général des lieux de privation de liberté (CPLG) indique dans un avis publié en 2011 « *qu'aucun accès aux services en ligne n'est possible ni en cellule, ni dans un local collectif surveillé* »[157] ; il souligne à nouveau dans son rapport d'activité pour l'année 2013, que le mot internet « *fait encore peur dans les établissements pénitentiaires même si des expériences de plateforme cyber-bases sont en cours dans quelques établissements.* »[158].

Il faut noter que depuis un décret du 20 mars 2003, les détenus peuvent acquérir du matériel informatique[159]. La circulaire de la Direction de l'Administration

[156] Voir pour ses régimes : les articles 39 et 40 de la Loi n°2009-1436 du 24 novembre 2009 pénitentiaire (1),

[157] Avis du contrôleur général des lieux de privation de liberté (Jacques Delerue) du 20 juin 2011 relatif à l'accès informatique des personnes détenues, JORF du 12 juillet 2011, texte 82 sur 134.

[158] Le contrôleur général ders lieux de privation de liberté, *Rapport d'activité 2013*, Paris : Editions Dalloz, 2014, 374pp., disponible sur le site du CGLPL : www.cglpl.fr

[159] Décret n°2003-259 du 20 mars 2003 modifiant le code de procédure pénale, qui crée l'article D.449-1. L'article est abrogé en 2013 ; il est refondu dans le règlement intérieur type des établissements pénitentiaires, inséré en annexe de l'article R.57-6-18 du CPP.

pénitentiaire en date du 13 octobre 2009 « *relative à l'accès à l'informatique pour les personnes placées sous main de justice* » précise toutefois que ce matériel informatique ne peut être communiquant, même dans le cas du matériel mis à disposition dans les salles d'activités encadrées[160]. D'une manière générale, l'administration précise que « *toutes les technologies permettant d'enregistrer ou d'envoyer des informations numériques vers l'extérieur de l'ordinateur sont interdites* »[161]. Le règlement intérieur type des établissements pénitentiaires, publié en annexe de l'article R.57-6-18 du Code de procédure pénale (CPP) tel qu'issu d'un décret du 30 avril 2013 dispose que l'action socioculturelle se fait par « *l'utilisation collective ou individuelle d'équipements informatiques non connectés à des réseaux extérieurs* »[162] et que « *l'utilisation ou la détention de téléphones portables ou de tout autre appareil communiquant est interdite* » [163].

66. **L'impossibilité d'un principe d'interdiction**. Or cette interdiction ne peut être affirmée tel un principe alors que la privation de liberté ne peut méconnaître le respect de la dignité et des droits du condamné[164]. L'exercice des droits du condamné ne peut faire l'objet d'autres restrictions que celles résultant des contraintes inhérentes à la détention, au maintien de la sécurité et au bon ordre des établissements, de la prévention de la récidive et de la protection de l'intérêt des victimes[165]. Deux problématiques apparaissent alors.

Dans un premier temps, eu égard au réseau envisagé comme un nouveau moyen de communication avec autrui, il faut considérer dans quelle mesure un accès au réseau peut permettre de concilier le respect du principe de libre communication avec autrui[166] et les restrictions inhérentes à la détention. Une analogie peut à ce niveau intervenir alors que le régime permettant aux détenus de communiquer avec autrui est depuis longtemps établi **(A)**. Dans un second temps, eu égard à l'application web qui permet non seulement un accès à l'information et une liberté d'expression mais également une liberté d'action, il faudra réfléchir à la conciliation entre la liberté d'accès au réseau

[160] Voir les principales technologies interdites classées dans un tableau *in Circulaire de la DAP en date du 13 octobre 2009 relative à l'accès à l'informatique pour les personnes placées sous la main de la justice*, Bulletin Officiel du Ministère de la Justice du 30 décembre 2009, justice 2009/6-Texte 16/33, page 6 et 8.

[161] *Ibid*., p.6

[162] V. : Décret n°2013-368 du 30 avril 2013 relatif aux règlements intérieurs types des établissements pénitentiaires et l'annexe de l'article R.57-6-18 du CPP.

[163] *Ibid*, article 27.

[164] Loi n°2009-1436 du 24 novembre 2009 pénitentiaire (1), article 22.

[165] *Ibid.*

[166] Le choix est ici fait d'utiliser la formulation « libre communication » pour désigner la liberté d'entrer en communication avec autrui et distinguer cette liberté de la liberté d'expression. De fait, l'article 11 de la Déclaration des Droits de l'Homme et du Citoyen fait référence aux deux libertés, ce qui conduit à fondre la communication avec autrui dans l'expression au public, ce qui nous semble dommageable à l'endroit du réseau et de son encadrement.

qu'il faut consacrer et les impératifs de la détention. La réflexion à cet endroit est nouvelle **(B)**.

A] La nécessaire mise en œuvre d'un accès au réseau en prison pour communiquer avec autrui

67. **Les relations des personnes détenues avec l'extérieur**. Le Code de procédure pénale dans sa partie règlementaire organise « *les relations des personnes détenues avec l'extérieur* »[167]. Il distingue les visites de la correspondance. Le droit à la correspondance est reconnu depuis longtemps aux détenus en application notamment de l'article 8 de la Convention Européenne des Droits de l'Homme[168]. Le droit à la correspondance écrite est ainsi mis en œuvre par l'article R.57-8-16 du CPP. L'accès au téléphone qui doit faire l'objet d'une autorisation du chef d'établissement pour les personnes détenues, est prévu par l'article R.57-8-16 du CPP. Ce droit à la correspondance ne se conçoit aujourd'hui que par la mise à disposition des détenus de ce nouveau moyen de communication qu'est le réseau. Les régimes de la correspondance écrite[169] et de l'accès au téléphone[170] peuvent de fait être transposés à la mise en œuvre d'une messagerie permettant l'échange de courriels.

68. **La création d'une messagerie dédiée au centre de détention et propre au détenu.** Il est tout à fait envisageable de mettre en œuvre un serveur informatique à l'échelle d'un centre de détention qui permettrait la création d'un service de messagerie dédié à celui-ci et qui pourrait dès lors faire l'objet d'une surveillance efficace au niveau de l'administrateur réseau[171]. Chaque détenu pourrait ainsi se voir allouer une adresse personnelle de type « jean.dupont@centrepénitentiairedefresne.fr **».** L'indication du centre de détention dans

[167] CPP, Partie règlementaire, Livre V « *Des procédures d'exécution* », Titre II « *De la détention* », Chapitre IX « *Des relations des personnes détenues avec l'extérieur* ».

[168] Golder c/ Royaume-Uni, 21 févr. 1975, *GACEDH*. Voir sur l'attention portée par le juge européen à l'égard de la correspondance des détenus : SUDRE Frédéric, *Droit européen et international des droits de l'homme,* 10ème. éd., Paris : P.U.F, 2010, point 294 « Le secret de la correspondance », 2°.

[169] CPP articles R57-8-16 à R57-8-19, l'article 39 de la loi n°2009-1436 du 24 novembre 2009 pénitentiaire (1) et la circulaire du 9 juin 2011 d'application des articles 4, 39 et 40 de la loi n°2009-1439 du 24 novembre 2009 pénitentiaire, relatifs à la correspondance téléphonique et à la correspondance écrite des personnes détenues, Bulletin officiel du Ministère de la justice et des libertés, BOMJL n° 2011-06 du 30 juin 2011.

[170] CPP articles R57-8-21 à R57-8-23, articles 40 de la loi n°2009-1436 du 24 novembre 2009 pénitentiaire (1), la circulaire de la DAP SD2 du 13 juillet 2009 relative à l'usage du téléphone par les personnes détenues condamnés, Bulletin Officiel du ministère de la justice, 30 Août 2004, justice 2009/4-Texte 41/51 et la circulaire du 9 juin 2011 d'application des articles 4, 39 et 40 de la loi n°2009-1439 du 24 novembre 2009 pénitentiaire, relatifs à la correspondance téléphonique et à la correspondance écrite des personnes détenues, Bulletin officiel du Ministère de la justice et des libertés, BOMJL n° 2011-06 du 30 juin 2011.

[171] Le vaguemestre aurait accès à l'ensemble des comptes des détenus et pourrait librement contrôler le contenu des messages.

l'adresse permet au destinataire ou à l'émetteur du courriel d'être informé du caractère particulier de celui-ci qui peut être soumis à contrôle[172].

Cet accès au service de messagerie pourrait se faire dans le cadre d'activités encadrées à des créneaux horaires décidés par l'administration pénitentiaire. A la différence de la correspondance écrite[173] et même si la limitation temporelle et spatiale d'accès au réseau limite de fait le nombre d'envois possibles, la facilité de communication permise par une messagerie électronique et surtout la volatilité et l'anonymat possible des adresses électroniques des destinataires de courriels pourrait conduire à limiter le nombre de destinataires possibles. Le régime établi pour les conversations téléphoniques pourrait être repris. Le détenu devrait ainsi soumettre au chef d'établissement une liste d'adresses de courriels qui nécessairement seraient nominatives. L'autorisation pour les membres de sa famille serait de droit. Cette liste pourrait être limitée à quarante adresses[174].

69. **De l'accès au téléphone à la communication par webcam**. Alors que le réseau permet désormais facilement à tous de mener une conversation avec un visuel, il pourrait être envisagé que le chef d'établissement autorise dans des circonstances familiales ou personnelles précises (maladie, éloignement important), la tenue d'une conversation via une webcam. Cette conversation, à l'instar d'une visite, se ferait sous la surveillance d'un agent[175] et pourrait, à l'instar d'une communication téléphonique, être écoutée, enregistrée et interrompue à tout moment[176].

B] L'interdiction de la navigation sur le web pour le détenu

70. **Le sens de la peine privative de liberté**. Au début des années 2010, la presse d'information générale notamment américaine dresse le portrait de détenus condamnés à des longues peines, qui n'ayant pas vécu l'émergence d'internet se trouvent concrètement confrontés à un choc technologique à leur sortie de prison. L'enfermement physique s'est

[172] Sur le contrôle possible de l'administration des courriers envoyés et reçus par le détenu : v. l'article 40 de la loi pénitentiaire de 2009, Loi n°2009-1436 du 24 novembre 2009 pénitentiaire (1).

[173] « *Les personnes détenues peuvent correspondre par écrit tous les jours et sans limitation avec toute personne de leur choix* », R57-8-16 CPP, alinéa 1.

[174] « *Le magistrat en charge de la procédure peut autoriser les personnes prévenues, détenues en établissement pénitentiaire ou hospitalisées, à téléphoner aux membres de leur famille ou à d'autres personnes pour préparer leur réinsertion*.», R57-8-21 CPP, alinéa 1. V. pour les modalités d'accès au téléphone, les circulaires mentionnées *supra*.
Une liste nominative et limitative de numéros de téléphone est établie. Elle est limitée à 40 numéros dans les établissements pour peine (20 numéros en maison d'arrêt en raison du « turn over » important des personnes détenues).

[175] Sur le régime du contrôle des visites, v. article D406 du CPP.

[176] Sur le régime du contrôle des conversations téléphoniques des détenus, v. article 727-1 du CPP. V. sur ce point des « visioconférences » en prison : Contrôleur général des lieux de privation de liberté, *Avis du contrôleur général des lieux de privation de liberté du 14 octobre 2011 relatif à l'emploi de la visioconférence à l'égard des personnes privées de liberté,* JORF du 9 novembre 2011.

doublé d'une privation d'accès à la technologie qui rend leur réadaptation à la vie en société encore plus difficile. Ce « choc » questionne l'interdiction de l'accès au réseau dans les prisons. Il est par ailleurs rappelé le contexte de l'introduction de la télévision dans les prisons françaises en 1985. Ce nouveau loisir qu'est internet ne peut être interdit aux détenus, qui ont aussi la « *triviale nécessité de passer le temps* »[177].

La revendication de l'introduction de l'accès à internet en prison s'inscrit de fait dans une conception nouvelle sur le sens et le but de la peine qui tend à humaniser la privation de liberté[178]. La peine consiste en l'enfermement physique du condamné et ne doit consister qu'en cela. Un double mouvement apparaît alors. Il faut d'une part défendre la conciliation des droits fondamentaux du condamné avec le régime d'enfermement[179] ; il faut d'autre part considérer davantage la nécessaire réinsertion du condamné qui serait soumis à une double peine si l'enfermement physique le conduisait à un enfermement social une fois sorti[180].

Sous ces deux angles, la privation de l'accès au réseau apparaît critiquable. Le caractère attentatoire aux libertés de la personne de cette interdiction générale d'accès a d'ailleurs était relevé par la Cour Européenne des Droits de l'Homme (CEDH) qui a sanctionné en janvier 2017 la Lituanie qui refusait à un détenu l'accès au réseau pour s'informer sur les conditions d'une formation à laquelle il souhaitait s'inscrire[181]. En France le CGLPL, en faveur d'une mise à disposition contrôlée d'internet, argue que le réseau est un « *vecteur de droits fondamentaux* » et que « *jamais un juge n'a condamné quelqu'un à être privé d'internet* »[182]. Dans une logique d'humanisation de la peine, il souligne d'abord la nécessaire protection des droits fondamentaux avant de souligner qu'ils ne peuvent être restreints que dans la limite du maintien de la sécurité, du bon ordre des établissements, de la prévention de la récidive et de l'intérêt des victimes[183].

La logique est donc celle de consacrer un droit d'accès pour ensuite limiter sa mise en œuvre eu égard aux possibilités que le réseau et ses applications permettent. Or s'agissant de l'application web, celle-ci permet d'être libre d'interagir avec le monde

[177] LECLERCQ Benjamin, « La prison déconnectée », article mis en ligne le 1er mai 2012, sur le site Owni.fr

[178] V. l'introduction du chapitre « Les condamnés en milieu fermé » *in* BOULOC Bernard, *Pénologie,* 3ème éd., Paris : Dalloz, 2005 (Précis), p. 179.

[179] V. : CEDH, 8 mars 1962, *Koch c/ RFA*, req. no 1270/61 et l'étude de Jean-Paul CÉRÉ, « Prison (normes européennes) », *Rép. Dalloz Dr. Pén. et Proc.pén*.

[180] Alors qu'en 1967, des auteurs (V. : SCHMELCK Robert et Georges PICCA, *Pénologie et droit pénitentiaire,* Paris : Éditions Cujas, 1967, p.129) soulignaient que « *l'accent de nos jours n'est plus mis sur l'expiation du coupable mais sur la défense de la société* », l'on pourrait aujourd'hui dire que l'accent n'est plus mis sur la défense de la société mais sur la réinsertion du condamné comme en témoigne la nouvelle rédaction de l'article 707 du code pénal.

[181] CEDH, AFFAIRE JANKOVSKIS c. LITUANIE, 17 janvier 2017, 21575/08.

[182] V. les propos de Jean-Marie Delerue rapportés *in* LECLERCQ Benjamin, « La prison déconnectée », *op. cit*.

[183] Contrôleur général des lieux de privation de liberté, *Avis du contrôleur général des lieux de privation de liberté du 20 juin 2011 relatif à l'accès à l'informatique des personnes détenues,* JORF du 12 juillet 2011, texte 82 sur 134.

extérieur dans une mesure telle que doit être posé le principe de l'interdiction de naviguer sur celui-ci.

71. **La privation de la liberté de naviguer sur le web**. Le verbe « naviguer » est révélateur de l'enjeu de l'accès à l'application web du réseau. L'individu peut se rendre sur tous les points du réseau et accéder à toutes les informations qui s'y trouvent. Deux problématiques apparaissent. D'une part, le détenu en naviguant n'a pas accès à un média classique qui vise son information ou son divertissement : il dispose d'un œil sur les agissements de tous. D'autre part, le propre du web est d'être devenu applicatif : il dispose d'une capacité d'interaction avec chacun[184]. Disant cela la privation de la navigation sur le web apparaît non pas comme la privation d'un loisir, ou comme une double peine mais bien comme le pendant naturel de la neutralisation que constitue la privation de liberté physique. Le principe doit être la privation de la capacité d'action eu égard au monde extérieur et ce pour des impératifs de sécurité et d'ordre public.

72. **L'impossible surveillance de la navigation sur le web**. En effet, il apparait difficile de concevoir la possibilité d'une navigation même pendant un temps limité et quand bien même celle-ci ferait l'objet d'une surveillance. Il faut relever le non-sens de la critique du CGLPL, qui dans son avis relatif à l'accès à l'informatique des personnes détenues, dénonce la prohibition de certains matériels de stockage en ces termes : « *certaines prohibitions de matériels limitant (de manière drastique eu égard aux normes actuelles) par exemple la capacité ou la puissance (ainsi pas de capacité de stockage des disques durs supérieure à 500Go), ne sont en rien liées aux mesures de sécurité à prendre mais seulement à la capacité de l'administration d'en contrôler l'usage ou le contenu. Autrement dit ce ne sont pas des considérations liées aux nécessités de l'ordre ou à l'intérêt des personnes qui président aux restrictions mais l'insuffisance des instruments de contrôle de l'administration* »[185].

Cette critique n'est pas recevable. L'humanisation de la peine trouve sa limite dans le contrôle que doit opérer en soi la privation de liberté physique. Il ne s'agit pas de permettre une liberté de stockage et d'échange de données entre les détenus, ou une liberté de navigation sur le web dès lors que celle-ci pourrait être enregistrée et

[184] Ainsi, en février 2015, un détenu du centre pénitentiaire de Béziers a mis en ligne sur son compte Twitter via l'application Périscope des vidéos de lui filmées dans sa cellule. Les vidéos qui le montraient un joint à la main ont été largement médiatisées ; une médiatisation qui montre la portée de l'audience de ce détenu qui dispose via son téléphone connecté à Internet non seulement d'une fenêtre sur le monde mais bien d'outil de communication. V. : « Un détenu placé en garde-à-vue après s'être filmé un joint à la main sur Periscope », *Lemonde.fr*, article mis en ligne le 22/02/2016, rubrique société.

[185] Contrôleur général des lieux de privation de liberté, *Avis du contrôleur général des lieux de privation de liberté du 20 juin 2011 relatif à l'accès à l'informatique des personnes détenues*, JORF du 12 juillet 2011, texte 82 sur 134.

contrôlée. L'impossibilité du contrôle ne tient pas à son coût matériel mais au sens même, dans le cas d'une détention, de donner plus de libertés qui nécessairement appellent à un contrôle.

73. **Le nécessaire filtrage du web**. Poser le principe de la privation de liberté de navigation ne veut pas dire que les détenus ne puissent pas avoir accès au web ; c'est la liberté d'usage qui est interdite, mais pas l'usage en lui-même. Le filtrage des sites accessibles à partir d'un centre de détention permet de concilier l'ouverture nécessaire sur le monde extérieur et les contraintes de sécurité et d'ordre public. Le contrôle s'opère préalablement à toute action du détenu, ce qui permet de délimiter les informations et les actions qui lui sont permises.

La mise en œuvre technique de ce contrôle est simple[186]. Le choix des critères du filtrage l'est moins. Actuellement, comme l'indique Corinne Peltier, coordinatrice de la Cyber-base® justice de la maison d'arrêt de Gradignan (Gironde), tous les sites sont interdits ; ils doivent donc être autorisés un à un. Elle témoigne de la procédure d'autorisation longue qui s'opère en six mois via une navette remontant jusqu'au ministère de la justice. Actuellement, plusieurs centaines de sites sont accessibles : « *de Wikipédia à la BBC, en passant par leboncoin.fr, Pôle emploi ou les Pages Jaunes. Tout site contenant des plans est en revanche recalé, à l'image de Mappy.com.* »[187]. Le filtrage pourrait aussi s'opérer par mots clefs qui seraient automatiquement refusés dans le cadre d'une recherche ; il est vrai alors que les limites seraient plus empiriques.

Il convient ainsi de mener une réflexion d'ensemble sur le filtrage du web dans les centres de détention, qui doit aller de pair avec une informatisation des prisons françaises[188]. Le droit fondamental à l'accès au réseau n'est pas méconnu en prison par le filtrage du web, il l'est par le manque de moyens[189] mis à disposition des détenus pour profiter d'un nouvel exercice des libertés qu'ils conservent dans la limite du contrôle que doit opérer leur enfermement.

---

[186] V. les propos de Mohamad Badras, chercheur au CNRS (Laboratoire Limos) et spécialiste de la sécurité internet, rapportés *in* LECLERCQ Benjamin, « La prison déconnectée », *op. cit*.

[187] V. les propos de Corinne Peltier, coordinatrice de la Cyber-base® justice de la maison d'arrêt de Gradignan (Gironde), rapportés *in* LECLERCQ Benjamin, « La prison déconnectée », *op. cit*.

[188] Voir sur ce point les initiatives mises en œuvre aux Etats-Unis qui introduisent des tablettes numériques spécifiques aux applications limitées dans les prisons. V. : RAWLINS Aimee, « How Philadelphia's prisons are embracing technology », article mis en ligne le 28 octobre 2014, sur le site de la chaîne d'information américaine CNN, rubrique « money », rubrique « small business », cnn.com

[189] Le rapport d'activité 2013 du contrôleur général ders lieux de privation de liberté indique qu'en 2011 la France comptait 11 cyber-bases®, *Rapport d'activité 2013*, Paris : Editions Dalloz, 2014, 374pp., disponible sur le site du CGLPL : www.cglpl.fr

74. **Transition**. Si l'on considère que la liberté d'accéder au réseau et de naviguer sur le web est un pendant de la sûreté personnelle, la privation de cette liberté en dehors de toute enfermement physique de la personne doit être entourée des mêmes garanties alors que la coupure d'accès prive l'individu de toute possibilité d'agir numériquement avec le monde qui l'entoure.

§2) Les conditions de la sanction pénale de la coupure d'accès au réseau

75. **Les conditions de la sûreté**. L'application de l'article 66 de la Constitution à la coupure d'accès au réseau permet d'en définir le régime. Alors que l'accès ne peut être arbitrairement coupé, il convient de réserver au législateur la détermination des infractions qui peuvent fonder une coupure d'accès au réseau **(A)**. La privation de liberté induite par la coupure d'accès doit être mise en œuvre par le juge judiciaire **(B)**.

A] Le respect du principe de la légalité pénale

76. **Les conditions de l'édiction d'une sanction pénale, privative de libertés**. Alors que la coupure d'accès prive l'individu de toute liberté d'action depuis son ordinateur ou son appareil électronique eu égard au monde extérieur, une telle privation ne peut être envisagée que dans le cas d'une sanction « pénale », du latin *poenalis, poena* : peine[190]. Eu égard à l'atteinte faite à la liberté de l'individu, elle ne peut être prononcée qu'au nom de la société en considération de la transgression d'une norme tenue pour essentielle[191].

Une telle sanction doit dès lors obéir au principe de la légalité des délits et des peines qui dans son adage latin énonce « *nullum crimen, nulla poena sine lege* ». Il figure à l'article 8 de la DDHC : « *La Loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une Loi établie et promulguée antérieurement au délit, et légalement appliquée*. ». Il est repris dans les « *principes généraux* » du Code pénal à l'article L111-3 : « *Nul ne peut être puni pour un crime ou un délit dont les éléments ne sont pas définis par la loi* ». Ce principe encadre la création d'une nouvelle infraction et de la peine qui y est associée.

Alors que la coupure de l'accès au réseau s'apparente à une privation de liberté physique, elle ne peut être prévue que par un texte de loi et sanctionner un crime ou un

[190] Voir l'entrée « pénal, ale, aux » *in* CORNU Gérard (*dir.*), Association Henri Capitant, *Vocabulaire juridique.* 10ème éd. Paris : P.U.F., 2014 (Quadrige).

[191] DREYER Emmanuel, Droit pénal général, 4ème éd., Paris : LexisNexis Litec (Manuel), 2016, p.1

délit **(1).** La peine doit par ailleurs être nécessaire, c'est-à-dire proportionnée à l'infraction qui la motive **(2)**.

1) Une peine délictuelle ou criminelle

77. **L'incidence du caractère technique et automatique de la coupure d'accès au réseau sur la nature de la peine**. Le caractère technique et automatique de la mise en œuvre d'une coupure d'accès au réseau se prête à une automatisation de la sanction. Elle est envisagée comme une réponse immédiate et facilement modulable dans le temps qui répond alors aux critères d'une peine contraventionnelle. Dans la droite ligne des nouvelles peines privatives ou restrictives de droit qui se sont substituées à l'amende au moment où l'emprisonnement était supprimé pour les contraventions de Vème classe[192], la suspension de l'accès apparaît comme une peine alternative à l'instar de la suspension du permis de conduire.

Il convient cependant d'affirmer que, eu égard à la nature de la privation de liberté opérée, la coupure d'accès au réseau quelque soit sa durée ne peut venir sanctionner qu'un crime ou un délit nécessairement défini par le législateur et non par le pouvoir règlementaire.

78. **Les différents cas de coupure d'accès prévus par la loi dite HADOPI 2 du 28 octobre 2009.** Il faut constater que la coupure d'accès n'a pour le moment été prévue que dans deux cas. La loi n°2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet[193] insère deux nouveaux articles dans le chapitre « Dispositions pénales » du Code de la Propriété Intellectuelle (CPI) qui définissent les cas où la coupure d'accès au réseau peut être mise en œuvre. L'un prévoit une peine délictuelle, l'autre une peine contraventionnelle.

Le nouvel article L335-7 du CPI prévoit que les délits de contrefaçon des articles L335-2, L335-3 et L335-4 lorsqu'ils sont commis au moyen d'un service de communication au public en ligne, peuvent être sanctionnés d'une peine complémentaire consistant en la suspension d'accès à un service de communication au public en ligne et l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur. La durée maximale de la coupure est d'un an.

[192] BOULOC Bernard, *Droit pénal général*, 23ème éd., Paris : Dalloz, 2013 (Précis), point 572.

[193] Loi n°2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, JORF du 29 octobre 2009, texte 1 sur 183.

Le nouvel article L335-7-1 du CPI énonce que les contraventions de Vème classe peuvent être, lorsque le règlement le prévoit, punies de la peine complémentaire de suspension de l'accès à un service de communication électronique dès lors qu'a été constaté une « *négligence caractérisée* » du titulaire de l'abonnement qui, averti de l'usage délictueux de son accès par la HADOPI, n'a pas mis en œuvre des moyens pour sécuriser son accès. La durée maximale de la coupure est d'un mois. C'est ici le défaut de sécurisation par l'abonné de son accès qui est sanctionné et non l'acte de contrefaçon.

La peine complémentaire de suspension d'accès au réseau de l'article L335-7 n'est pas critiquable au regard du principe de légalité alors qu'elle vient sanctionner des délits. Il faudra simplement s'interroger sur la nécessité d'une telle sanction. En revanche, l'article L335-7-1 ne peut perdurer alors qu'une telle coupure ne peut être décidée par le pouvoir règlementaire.

79. **La nécessaire suppression de la peine contraventionnelle de suspension d'accès.** Un décret du 25 juin 2010[194] vient définir la contravention de négligence caractérisée punie d'une amende de la cinquième classe, qui peut donc en application de l'article L335-7-1 faire l'objet d'une peine complémentaire de suspension de l'accès pour une durée maximale d'un mois. Cette contravention est définie à l'article R335-5 du CPI.

La problématique ici n'est pas celle des contours de la définition de cette nouvelle infraction qui vise le titulaire de l'abonnement ; ni même celle du bien-fondé de la création d'une telle infraction[195]. Ce qui pose problème ici est l'inadéquation entre la l'objet de la sanction et la nature de l'infraction. Alors que l'accès au réseau renvoie à la liberté individuelle du citoyen, le pouvoir règlementaire ne peut définir les conditions de la coupure d'accès au réseau dans le cadre d'une infraction contraventionnelle. Il n'a pas le pouvoir de décider d'une telle privation de liberté.

De fait, alors qu'en 2012 s'opère un changement de majorité politique, un décret du 8 juillet 2013[196] vient supprimer la peine complémentaire de suspension de l'accès à un service de communication au public en ligne dans le cas de la contravention de négligence caractérisée de la part du titulaire de l'abonnement ; seule l'amende prévue pour les contraventions de cinquième classe subsiste. Cette suppression est à saluer. Il

[194] Décret 2010-695 du 25 juin 2010 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur internet, JORF du 26 juin 2010, texte 11 sur 122.

[195] V. : IMBERT-QUARETTA Mireille et al, « La contravention de négligence caractérisée à la lumière de la mise en œuvre de la procédure de réponse graduée », *JCP G*, n°19, 7 mai 2012, étude n°591.

[196] Décret n° 2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle, JORF du 9 juillet 2013, texte 9 sur 160.

conviendrait toutefois de supprimer du CPI l'article L335-7-1 qui continue d'énoncer que le pouvoir règlementaire est fondé à mettre en œuvre à titre de peine complémentaire une suspension d'accès.

2) Une peine nécessaire

80. **Une privation de libertés**. Le caractère technique et automatique de la coupure d'accès ne doit pas venir minimiser son incidence pour le citoyen. Il s'agit d'une véritable privation de libertés. L'individu ne peut plus exercer depuis son domicile ou grâce à son mobile l'ensemble des libertés qui lui sont reconnues dans un État de droit : celle d'entrer en communication avec autrui, de commercer, d'échanger, de s'informer, de s'exprimer, de se divertir.

Il faut condamner les raisonnements assez fréquents[197] qui viennent minimiser les conséquences d'une coupure d'accès. Ainsi Bertrand de Lamy énonce : « *Encore est-il possible d'opposer que l'intéressé aurait pu utiliser la connexion d'un membre de sa famille, d'un voisin, d'un cybercafé ou existant sur son lieu de travail. Un internaute se voyant simplement privé de l'accès à la toile à partir de la seule ligne ouverte à son nom voit sa liberté beaucoup moins restreinte, par exemple, qu'un automobiliste dont le permis a été invalidé*. »[198]. Cette argumentation ne convainc pas. Un automobiliste privé de son permis peut tout aussi bien se faire conduire par un membre de sa famille ou un collègue, ou prendre les transports en commun. La sanction ne réside pas dans la privation du moyen de transport ou d'accès au réseau mais bien dans la liberté d'usage de celui-ci.

Or il faut considérer la forte restriction dans l'usage qui peut être fait du réseau qui pèse sur l'individu s'il ne peut plus y accéder depuis son domicile ou son mobile. L'individu est contraint par des horaires, par un déplacement vers un point de connexion, qui peut être l'objet d'une surveillance comme celle fournie par son employeur ou faire l'objet d'un paiement comme celle d'un cybercafé. L'accès peut aussi, tout simplement, ne pas être relié à une imprimante ce qui peut être problématique pour diverses formalités. Le Conseil constitutionnel souligne justement cet enjeu dans sa

[197] Ainsi des propos de Christine Albanel lors de son audition le 17 février 2009 dans le cadre de l'examen, en première lecture devant l'Assemblée Nationale du projet de loi Hadopi 1. Interrogée sur l'amendement du député Guy Bono introduit devant les instances européennes et visant à faire du droit à l'accès au réseau, un droit fondamental, la ministre de la culture répond que « *l'accès est possible ailleurs, chez un ami ou un voisin alors que celui qui est privé de son permis de conduire ne peut plus du tout prendre le volant. Le recours devant un juge est possible. Les FAI prennent au demeurant très souvent une telle sanction à l'encontre de clients qui ne paient pas leurs abonnements sans que cela ne provoque de réaction.* » V. : Le dossier législatif du Projet de loi favorisant la diffusion et la protection des œuvres sur internet, n°405, déposé en première lecture au Sénat le 18 juin 2008.

[198] LAMY de, Bertrand, « HADOPI 1 : Précisions du Conseil constitutionnel sur le pouvoir de punir », *RSC* 2010, n°209.

décision du 10 juin 2009 (Loi Hadopi 1) dans son considérant 16, lorsque, pour censurer le pouvoir de la Hadopi eu égard à la coupure d'accès, il renvoie au droit de s'exprimer et de communiquer librement « *notamment depuis son domicile* »[199]. Il y voit ainsi une circonstance aggravante ; l'accès à domicile ne peut être envisagé comme une « commodité »[200]. La liberté d'accès ne se réalise que dans l'intimité de son foyer et une coupure d'accès ne peut être motivée que par une infraction justifiant une telle privation de liberté.

81. **Les infractions pouvant justifier une coupure d'accès**. Tout crime ou délit sanctionné par une peine d'emprisonnement peut se voir adjoindre la peine complémentaire de coupure d'accès au réseau. Elle peut ainsi permettre de sanctionner de manière adéquate un comportement grave qui n'emporte toutefois pas la mise en œuvre d'une peine d'emprisonnement qui serait nécessairement de courte durée.

Ainsi cette peine mise en œuvre par l'article L335-7 du CPI qui vise les délits de contrefaçon des articles L335-2, L335-3 et L335-4 est tout à fait justifiée alors que ces délits sont sanctionnés de 3 ans d'emprisonnement et de 300 000 euros d'amende. Elle ne peut toutefois intervenir que si elle s'avère proportionnelle à l'infraction constatée comme l'énonce l'article L335-7-2 du CPI : « *Pour prononcer la peine de suspension prévue aux articles L. 335-7 et L. 335-7-1 et en déterminer la durée, la juridiction prend en compte les circonstances et la gravité de l'infraction ainsi que la personnalité de son auteur, et notamment l'activité professionnelle ou sociale de celui-ci, ainsi que sa situation socio-économique. La durée de la peine prononcée doit concilier la protection des droits de la propriété intellectuelle et le respect du droit de s'exprimer et de communiquer librement, notamment depuis son domici*le. ». La coupure d'accès apparaît ainsi comme une alternative à l'emprisonnement mais ne peut consister en une sanction faisant l'objet de gradations renvoyant aux atteintes subies. C'est l'intérêt général qui commande son édiction et non la prise en compte du préjudice personnel ressenti par la victime[201].

Elle peut également venir sanctionner d'autres délits graves comme le préconise le rapport sur la cybercriminalité intitulé « Protéger les internautes » du groupe de

[199] Conseil constitutionnel, décision n°2009-580DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, JORF du 13 juin 2009, p.9675.

[200] MARINO Laure, « Le droit d'accès à Internet, nouveau droit fondamental », *D.*2009 n°30, Point de vue, p.2046.

[201] Ainsi la sanction d'un ou plusieurs mois de suspension ne peut être fonction du nombre de titres téléchargés par exemple mais doit s'inscrire dans une appréciation plus large qui prend en compte l'incidence de l'acte eu égard à la société. Ainsi une telle suspension d'accès pourrait être envisagée dans le cas de la création d'un site permettant le téléchargement de plusieurs œuvres contrefaites qui seraient monnayées aux tiers.

travail interministériel sur la lutte contre la cybercriminalité de février 2014[202]. Ainsi ce rapport prévoit d'ériger la coupure d'accès à un réseau de communications électroniques en peine complémentaire pour les infractions commises au moyen d'un tel réseau et mettant en péril un mineur soit sous la forme de propositions sexuelles (art. 227-22-1 du Code pénal), soit par le biais de la pédopornographie (art. 227-23), soit au titre des atteintes sexuelles dans l'hypothèse prévue par l'article 227-26 al. 4 du même code[203].

82. **La difficile mise en œuvre d'une telle sanction**. Evidemment, la mise en œuvre d'une telle coupure doit être effective. C'est à ce niveau qu'une telle sanction apparaît difficile à mettre en œuvre. Il pourrait être notifié à tous les opérateurs l'interdiction faite à un individu de s'abonner au réseau, ce qui n'empêcherait pas l'abonnement opéré par un tiers. L'adresse du domicile de l'individu pourrait faire l'objet d'une liste noire interdisant aux opérateurs tout raccordement au réseau. Toutefois cette sanction viendrait alors toucher l'ensemble des individus vivant au foyer de l'auteur de l'infraction, ce qui ne peut être.

B] La compétence exclusive du juge judiciaire

83. **Plan**. La décision de couper l'accès à un individu ne peut relever que du juge judiciaire, un principe qui n'est pas reconnu actuellement par les textes **(1)**. Dès lors, alors que dans le contexte de la lutte contre le terrorisme, la coupure administrative d'accès au réseau est aujourd'hui envisagée, il convient de souligner qu'il s'agit d'une atteinte grave à la sûreté qui questionne sa nécessité et les modalités de sa mise en œuvre **(2)**.

1) Le juge de la privation de liberté

84. **Le sort de l'amendement dit « Bono » devant le Parlement européen**. Le 10 avril 2008, dans le cadre de la révision du Paquet télécom, le Parlement européen émet une résolution « sur les industries culturelles en Europe » qui engage les États membres « *à éviter l'adoption de mesures allant à l'encontre des droits de l'homme, des droits civiques et des principes de proportionnalité, d'efficacité et d'effet dissuasif, telle que l'interruption d'accès à internet* »[204]. Le 6 mai 2009, le député européen Guy Bono, lors de la première lecture de la directive modifiant la directive cadre, introduit l'amendement 138 qui va dans le sens de la

[202] Le rapport est disponible à cette adresse : http://www.justice.gouv.fr/la-garde-des-sceaux-10016/lutte-contre-la-cybercriminalite-27255.html

Le groupe de travail interministériel chargé d'élaborer une stratégie globale de lutte contre la cybercriminalité et présidé par le Procureur général Marc Robert a remis son rapport le 30 juin 2014, aux ministres Christiane Taubira, Arnaud Montebourg et Bernard Cazeneuve et à la secrétaire d'Etat au Numérique Axelle Lemaire.

[203] Voir la recommandation n°10 relative à la peine complémentaire de suspension du droit d'accès à Internet, p.158 du rapport.

[204] V. : « En bref », *RLDI* 2008/37, p.21. La résolution est disponible sur le site du Parlement européen : http://www.europarl.europa.eu/

résolution du Parlement : « *Aucune restriction aux droits et libertés fondamentales des utilisateurs finaux ne doit être prise sans décision préalable de l'autorité judiciaire en application notamment de l'article 11 de la Charte des droits fondamentaux* »[205]. Cet amendement est voté à une forte majorité et fait craindre en France à une mort prématurée du projet de loi Hadopi[206].

De fait le contenu de cet amendement rejoint la position prise quelques jours plus tard par le Conseil constitutionnel français qui réserve à l'autorité judiciaire le pouvoir de couper l'accès au réseau de l'internaute. Malheureusement cet amendement dit « Bono » va souffrir du contexte politique qui l'entoure et qui oppose les tenants d'un internet dit « ouvert » et les défenseurs du droit d'auteur. Il n'est pas repris dans la directive cadre telle que modifiée en 2009. La formulation finale qui entoure les mesures visant l'accès des utilisateurs est générale et ne permet pas d'appréhender quelles sont les libertés et les droits fondamentaux concrètement en jeu[207].

La démarche de l'amendement « Bono » a souffert ici encore de ses contours peu délimités qui ont fait craindre à un droit à l'accès absolu et à une interdiction générale du contrôle des contenus. Or si le droit d'accès est défini comme la liberté pour un individu d'accéder au réseau et non comme la liberté de laisser être diffusés tous les contenus, on ne peut que considérer, comme cette section l'a montré, que seul le juge judiciaire peut être investi du pouvoir de restreindre cette liberté.

2) L'interdiction d'une coupure administrative de l'accès

85. **La difficile justification d'une coupure administrative de l'accès au réseau.** Si la privation de liberté neutralise l'individu, elle ne le fait que dès lors qu'il a commis une infraction définie. Elle se distingue d'une mesure de police qui a pour but de prévenir le

[205] V. : « Actualités, Eclairage », *RLDI* 2008/42, p.7.

[206] GIRARDEAU Astrid, « L'Europe étourdit Hadopi », article mis en ligne le 7 mai 2009 sur le site du journal Libération, rubrique « médias », www.libération.fr

[207] V. : la directive 2009/140/CE du 25 novembre 2009 du Parlement européen et du Conseil modifiant la directive « cadre », la directive « accès » et la directive « autorisation ». Son article 1Er modifie l'article 1er de la directive CADRE comme tel : « *Le paragraphe suivant est inséré : « Les mesures prises par les États membres concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques respectent les libertés et droits fondamentaux des personnes physiques, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les principes généraux du droit communautaire.*

Toute mesure susvisée concernant l'accès des utilisateurs finals aux services et applications, et leur utilisation, via les réseaux de communications électroniques qui serait susceptible de limiter les libertés et droits fondamentaux précités ne peut être instituée que si elle est appropriée, proportionnée et nécessaire dans le cadre d'une société démocratique, et sa mise en oeuvre est subordonnée à des garanties procédurales adéquates conformément à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et aux principes généraux du droit communautaire, y compris le droit à une protection juridictionnelle effective et à une procédure régulière. Par voie de conséquence, les mesures en question ne peuvent être prises que dans le respect du principe de la présomption d'innocence et du droit au respect de la vie privée. Une procédure préalable, équitable et impartiale est garantie, y compris le droit de la ou des personnes concernées d'être entendues, sous réserve de la nécessité de conditions et de modalités procédurales appropriées dans des cas d'urgence dûment établis conformément à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Le droit à un contrôle juridictionnel effectif en temps utile est garanti.».

trouble à l'ordre public. Or, alors que la régulation des contenus diffusés peut apparaître difficile, il est tentant pour prévenir le trouble à l'ordre public, non plus de supprimer l'information disponible, mais d'agir au niveau de l'individu pour empêcher celui-ci d'y avoir accès.

Ainsi dans le cadre de la discussion du projet de loi renforçant la lutte contre le terrorisme[208], un amendement a été déposé qui prévoyait la suspension de l'accès au réseau pour une durée minimum de 5 ans dans le but de « *de prévenir toute consultation de sites internet appelant à la commission d'actes de terrorisme ou fournissant des techniques permettant le passage à l'acte et qui seraient toujours consultables malgré l'adoption de la présente loi*. »[209]. Si l'amendement n'a pas été soutenu[210] devant l'Assemblée, sa simple formulation mérite qu'on s'y arrête alors qu'il envisage la coupure d'accès en ces termes : « *Il est établi une liste noire de l'ensemble des ressortissants français, y compris mineurs, qui projettent des déplacements à l'étranger ayant pour objet la participation à des activités terroristes, des crimes de guerre ou des crimes contre l'humanité, ou sur un théâtre d'opérations de groupements terroristes, auprès de tous les fournisseurs internet présents sur le territoire national afin que ceux-ci suspendent leur connexion pour une durée minimum de cinq ans. La régularité de l'établissement de cette liste est soumise au contrôle d'un magistrat judiciaire. ».*

86. **Le caractère liberticide de la coupure administrative de l'accès au réseau**. La mention du « *contrôle d'un magistrat judiciaire* » ne suffit pas ici à garantir contre l'arbitraire alors que la coupure vise un individu qui « projette » un déplacement à l'étranger et une participation à un acte terroriste. Cette sanction ne peut par ailleurs avoir lieu dans un État de droit alors qu'elle s'apparenterait à une détention préventive pouvant aller jusque 5 ans alors qu'aucune infraction n'a été constatée. Il faudrait à cet endroit reprendre l'ensemble des propos introductifs du professeur Georges Burdeau dans le cadre d'une section intitulée « *Les restrictions à la sûreté individuelle motivées par l'intérêt public* » qui sont remarquables. Peut être cité le paragraphe concluant ces propos : « *Ainsi la détention par mesure administrative est une de ces institutions que leur utilité défend mieux que leur justification*

[208] Projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, n° 2110, déposé le 9 juillet 2014 et renvoyé à la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République. Le dossier législatif est disponible sur le site de l'Assemblée nationale, http://www.assemblee-nationale.fr/

[209] V. L' exposé sommaire de l'amendement n°73 présenté par M. Estrosi, M. Sermier, M. Hetzel, M. Saddier, M. Morel-A-L'Huissier, M. Jean-Pierre Vigier, M. Alain Marleix, M. Furst, M. Ginesy, M. Suguenot, M. Vitel, M. Olivier Marleix, M. Siré, M. Huet, M. Chartier et M. Dord. V. le dossier législatif du projet de loi.

[210] « *Un amendement non défendu par son auteur ou par l'un de ses cosignataires absents en séance lors de son appel est considéré comme « non soutenu ». À l'Assemblée nationale, il ne peut pas être repris par le Gouvernement*. », V. le point « 2.2.4 Discussion parlementaire des projets de lois » du guide de légistique disponible sur le site www.légifrance.gouv.fr.

rationnelle. Avec l'internement administratif on peut se demander si l'efficacité même de la mesure est réelle. Destinée à mettre hors d'état de nuire des individus présumés dangereux pour la sécurité de l'Etat, son effet le plus sûr, au dire de certains, serait de rendre effectivement dangereux les innocents qu'elle a frappés. Dès lors mieux vaudrait supprimer une institution qui, moralement répréhensible, ne peut même pas se réclamer de son utilité pratique »[211].

Si une telle coupure d'accès préventive ne peut être mise en œuvre dans un État démocratique, la formulation d'une telle possibilité est révélatrice du mouvement actuel qui tend à vouloir limiter ou contrôler la liberté d'agir de l'individu en utilisant les caractéristiques techniques du réseau, alors pourtant que c'est le réseau qui doit être contraint pour sauvegarder la liberté individuelle de la personne.

[211] Georges BURDEAU, *Libertés publiques*, 4ème éd., Paris : Librairie générale de droit et de jurisprudence, 1972, p.161.

Conclusion Chapitre 2ème

87. **Le rattachement par le Conseil constitutionnel de la liberté d'accès à la liberté de communication garantie à l'article 11 de la DDHC**. Les débats autour de la reconnaissance d'une liberté d'accès au réseau ont eu lieu dans le cadre de la lutte contre le téléchargement illégal alors que la coupure d'accès au réseau était envisagée comme une sanction à un acte de contrefaçon et même comme une sanction au défaut de sécurisation de l'accès à internet par son titulaire.

Dans sa décision du 10 juin 2009 s'agissant de la « loi favorisant la diffusion et la protection de la création sur internet » et instituant la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet (dite « HADOPI »), le Conseil constitutionnel rattache la liberté d'accéder au réseau à la liberté de communication garantie par l'article 11 de la DDHC. Dès lors, de même valeur que le droit de propriété intellectuelle qui assure la protection des auteurs, une mise en balance aurait dû s'opérer.

Toutefois le Conseil énonce que cette sanction de la coupure d'accès,- dont il est prévu qu'elle ne dure qu'un mois pour un défaut de sécurisation-, ne peut être le fait de la HADOPI qui n'est pas une juridiction alors qu'elle conduit « *à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile* ». Une position qui questionne les commentateurs alors que le Conseil constitutionnel a depuis longtemps reconnu que des sanctions pouvaient être prises par les autorités administratives tant qu'elles n'étaient pas privatives de liberté et qui semble de fait hiérarchiser des libertés de même ordre.

88. **Le possible rattachement à la liberté individuelle de l'article 66 de la Constitution**. En réalité il ne peut s'agir de graduer une coupure d'accès en fonction de l'acte réprimé. La coupure d'accès prive l'individu de l'exercice de l'ensemble de ses libertés qui trouvent leur prolongement de manière dématérialisée sur le réseau. La liberté d'accès au réseau est le pendant de la liberté individuelle.

Reprenant la formulation de l'article 66 de la Constitution, l'on pourrait ainsi énoncer que : « *Nul ne peut être arbitrairement privé de son accès à un réseau de communications électroniques. L'autorité judiciaire, gardienne de la liberté d'accès au réseau, assure le respect de ce principe dans les conditions prévues par la loi* ». Cette

affirmation fait de l'accès au réseau, une liberté de premier ordre au sens où elle conditionne la mise œuvre de toutes les autres libertés telles que la liberté d'expression, la liberté de commercer ou encore la liberté de travailler; ce qui pourtant n'en fait pas un droit général ou absolu alors que l'individu peut être privé de cet accès de la même manière qu'il peut être privé de sa liberté physique en étant enfermé, et que par ailleurs les activités mises en œuvre sur le réseau doivent faire l'objet d'une règlementation.

89. **Les conditions de la privation d'accès au réseau**. Envisager la liberté d'accès au réseau et sa privation en opérant une analogie avec la liberté individuelle et la privation de liberté physique de l'individu, permet de réfléchir utilement au régime de l'accès au réseau dans les prisons, qui au-delà des contraintes budgétaires pour informatiser celles-ci, peine à émerger. Entendu comme un nouveau moyen de correspondances privées grâce aux courriels et aux webcams, une analogie avec les régimes actuels de contrôle des courriers et des communications téléphoniques est tout à fait opérant. En revanche s'agissant de l'accès au web, l'affirmation d'un droit d'accès au réseau dans les prisons ne peut équivaloir à une liberté de naviguer sur la toile ; une limitation des sites accessibles est nécessaire pour réaliser la neutralisation du détenu.

Par ailleurs, en dehors de toute détention physique de l'individu, une suspension de l'accès au réseau peut être considérée. Elle ne peut toutefois être la sanction que d'une peine délictuelle ou criminelle. En ce sens il faut saluer que depuis 2012, il n'est plus de peine contraventionnelle de suspension de l'accès visant la négligence caractérisée du titulaire de l'abonnement au réseau. De plus cette suspension ne peut être le fait que du juge judiciaire et il faut être vigilant s'agissant de toute dérive sécuritaire visant à envisager la suspension d'accès à un individu présumé dangereux en dehors de tout constat d'une infraction. Ce n'est pas à l'individu d'être privé préventivement d'accès mais bien au réseau d'être gouverné.

CONCLUSION TITRE I

90. **La consécration d'une nouvelle liberté publique.** Il est choisi ici de ne pas adopter la formulation d'un « droit d'accès au réseau » mais d'une liberté d'accès à celui-ci. En effet, la formulation d'un « *droit à* » nous parait aujourd'hui difficilement dissociable du contexte tendu qui a vu l'émergence de ce concept et des inquiétudes autour d'un droit-créance aux contours non définis. L'approche n'est pas subjective dans sa formulation mais renvoie au mécanisme d'une liberté publique qui consacre à l'égard de chacun un espace de liberté.

Celui-ci doit être garanti par la mise en œuvre d'un service public de l'accès qui s'entend de l'accès à la structure du réseau et de la promotion de l'insertion numérique. Il implique également que soit défini un régime qui vise les exigences d'un tel service, alors que le traitement des connexions par les opérateurs ne peut être soumis aux aléas d'une économie de marché et qu'un minima de débit et de services soit garanti à tous.

Cette liberté d'accès doit être reconnue comme une liberté de premier ordre. Elle est le nouveau pendant de la sûreté individuelle eu égard à la capacité d'action avec le monde extérieur que permet l'accès au réseau. L'enjeu de cette liberté fonde un régime effectif qui la délimite. A l'instar de l'emprisonnement d'un individu, l'accès au réseau ne peut être arbitrairement coupé. La loi doit prévoir cette sanction dans le cadre de la définition de peines délictuelles ou criminelles. Cette privation d'accès ne peut être décidée que par le juge judiciaire.

Le régime de la liberté d'accès défini, il faut alors envisager dans un second temps celui de la liberté de naviguer sur le web.

TITRE II. LA LIBERTE DE NAVIGUER SUR LE WEB

91. **L'enjeu du contrôle de la structure du réseau**. Dans une logique de territorialisation du réseau, la liberté d'accès au réseau doit également s'entendre une fois l'accès physique au réseau garanti comme la liberté de naviguer entre tous les points du réseau qui est mondial. Le principe de neutralité se prolonge ainsi dans l'abstention qui doit être celle d'un État de droit eu égard au contrôle des voies de communication. Un État démocratique ne peut arbitrairement agir sur la structure du réseau pour empêcher la communication entre deux points de celle-ci. Il convient de considérer que la coupure d'accès à certains serveurs ou sites ne s'apparente pas à une atteinte à la liberté d'expression mais renvoie à la réalité concrète d'un territoire et au contrôle des déplacements des citoyens d'un État.

La liberté de naviguer sur le web s'inscrit dans le prolongement de la liberté de circulation de l'information ou « *free flow of information* » reconnue dans les années 1980 et qui a justifié une protection des personnes s'agissant des traitements de données qui pouvaient les concerner. La transmission de données n'est plus le fait aujourd'hui de systèmes automatisés statiques relevant des États ou d'entreprises privées mais s'opère essentiellement à travers ce nouveau moyen de communication qu'est le réseau. La problématique dès lors ici dans un premier temps ne vise pas l'intégrité de la personne humaine et le fichage qui pourrait découler du traitement de telles données mais le contrôle immédiat et automatique de l'individu s'il était empêché d'agir par une action technique annihilant directement une partie de ses capacités d'action sur le réseau.

92. **La liberté de naviguer vers tout point du réseau de communication et non la liberté de diffuser tout contenu**. Ce qu'il faut condamner est l'action sur la connexion en elle-même qui serait empêchée d'accéder aux contenus par le contrôle des voies de communication et non la mise en œuvre d'un régime qui viserait les contenus et pourrait opérer une régulation de leur diffusion selon des mécanismes démocratiques éprouvés.

En effet, toute action technique sur le routage des connexions ou sur les serveurs stockant les données mises en ligne, autrement dit toute action sur la manière dont l'individu peut se diriger sur le réseau, souffre moins de nuances qu'une police des contenus diffusés et une suppression à la source des contenus sanctionnés. En agissant

sur la demande et sur la possibilité qu'elle a d'accéder aux différents points du réseau, c'est l'ensemble d'un site du web ou d'un service comme un moteur de recherche ou un réseau social, qui peut techniquement être bloqué.

Dès lors, l'individu est empêché d'agir plus qu'il n'est empêché de s'informer. Le contrôle des voies de communication permet ainsi à des régimes autoritaires de faire d'internet un réseau local limité aux seules connexions à l'intérieur du pays. Un contrôle qui *in fine* limite les contenus disponibles mais qui renvoie d'abord à une fermeture des frontières. Ainsi le filtrage qu'opèrent les régimes autoritaires renvoie à la réalité d'un territoire et à des enjeux géopolitiques. Fermer le site d'un dissident chinois est une atteinte à la liberté d'expression qu'une société démocratique doit protéger ; limiter l'accès d'un internaute aux sites de la boucle locale du réseau qui couvre le territoire national est une atteinte à la liberté de naviguer sur le web qu'une société démocratique doit également garantir.

93. **Les deux aspects de la liberté de naviguer sur le réseau**. Ainsi à l'instar de la liberté d'aller et venir, la liberté de naviguer sur le réseau englobe deux libertés distinctes[212]. La première concerne le principe même de déplacement sur le réseau, c'est-à-dire l'accès à tous les points du réseau. Un principe auquel on ne peut porter atteinte d'une manière telle qu'est annihilée liberté de choix de l'internaute dans ses connexions et donc sa liberté individuelle. Dès lors le régime du blocage d'un site doit être celui d'une police administrative spéciale (**Chapitre 1er**). La seconde liberté réside, une fois tous les points du réseau accessibles, dans la possibilité de consulter tous les sites et services disponibles sur le web. Cette liberté peut souffrir des limitations mais qui doivent être encadrées (**Chapitre 2ème**).

Chapitre 1er. Le régime du blocage d'un site, restriction à la liberté de naviguer

Chapitre 2ème. La règlementation des limitations à la consultation de certains sites et services

[212] RIVERO J., MOUTOUH H. *Libertés publiques,* Tome I, 7ème éd., Paris : P.U.F. Droit (Thémis, droit public), p.101.

Chapitre 1er : Le régime du blocage d'un site, restriction à la liberté de naviguer

94. **L'analogie avec la liberté d'aller et venir**. Une analogie peut être établie avec la liberté d'aller et venir. Ce qui est visé ici n'est pas le déplacement de l'individu mais la transmission de sa demande sur le réseau. Celle-ci doit pouvoir atteindre l'ensemble des points du réseau, c'est-à-dire l'ensemble des serveurs qui hébergent les différents services de communication du réseau (serveurs d'annuaires de noms de domaine, de messageries, de P2P, de services et sites du web).

La difficulté est qu'internet étant un réseau informatique, il est difficile de définir le critère de l'extranéité et dès lors de fonder un rapport de souveraineté. Le maillage du réseau n'est pas le fait des États mais relève du développement des services mis en œuvre par des entreprises privées[213] ; l'adressage et le nommage du réseau sont le fait d'une organisation internationale[214]. Dès lors la composante de la liberté d'aller et venir qui vise l'entrée et la sortie d'un territoire n'a pas lieu d'être. La raison d'être du réseau internet est l'internationalité de la communication qu'il permet. La définition d'une frontière ne peut être le fait que d'un acte de souveraineté, extérieur au réseau, qui dès lors contraint la structure selon ses propres critères ce qu'il faut condamner alors que cela annihile la liberté de choix des internautes.

95. **Le principe de la libre navigation de l'internaute**. Subsiste toutefois la liberté de circulation des internautes, liberté qui renvoie à leurs choix de consultation sur le réseau. Cette liberté est violée par les tentatives de régimes autoritaires qui souhaitent limiter les communications à l'intérieur du pays en limitant l'accès de leurs citoyens à un ensemble de services et de sites selon des critères arbitraires qui relèvent d'une idéologie politique. Le principe dans un Etat démocratique doit être celui d'une libre navigation de l'internaute alors qu'est reconnu à l'individu le droit de circuler sur le territoire national et le droit de quitter celui-ci ; droits qui, ici, se confondent alors que l'internationalité du réseau en fait un espace unique.

[213] Qui acquièrent physiquement des fermes de serveurs au fur et à mesure de leurs besoins en termes de trafic et de stockage.

[214] L'ICANN pour « *Internet Corporation for Assigned Names and Number* » est une organisation internationale sans but lucratif créée aux Etats-Unis en 1998. V. : pour le détail des ses fonctions, *infra* n°208 et suiv.

Il faut cependant insister sur le fait qu'un État démocratique ne peut garantir cette liberté qu'en se réservant la possibilité de bloquer certains sites ou services. En effet il faut opposer aux partisans d'un internet dit *« libre* » qu'une telle dérégulation conduit à l'asservissement de l'internaute alors que si le réseau n'est pas gouverné, c'est dès lors sur l'individu que la contrainte étatique va peser. L'État est tenté de mettre en œuvre une surveillance générale de ses faits et gestes. Ce qu'il faut condamner en restaurant un régime effectif de régulation des services accessibles sur le réseau.

96. ***Plan.*** Il faut ainsi affirmer la nécessité de la mise en œuvre de mesures de blocage dans un État démocratique (**Section I)** et dès lors considérer le régime de cette mesure qui ne peut être que de police administrative spéciale (**Section II).**

Section I. La nécessité des mesures de blocage dans un état démocratique

97. **Le caractère de la liberté de naviguer sur le web.** La liberté de naviguer sur le web est « *absolue* »[215], ou encore « *spontanée* »[216] ou « *naturelle* »[217] pour employer les épithètes donnés à la liberté d'aller et venir du national. Elle se réalise par le seul accès au réseau : l'État n'a pas d'obligations positives à mettre en œuvre pour que celle-ci se réalise dès lors qu'il a mis à disposition de l'individu un accès faisant l'objet d'obligations de service public. Elle est absolue dès lors que ce choix de navigation n'emporte aucune conséquence matérielle. Personne ne peut être tenu responsable de la navigation opérée[218]. C'est n'est pas à l'individu d'être surveillé et contraint mais au réseau d'être gouverné.

Ainsi ce caractère spontané et absolu de la liberté de naviguer sur le web fait apparaître que si la sélection des sites accessibles aux nationaux est nécessairement autoritaire **(§1),** il est nécessaire en revanche dans un État de droit que le réseau soit gouverné par la mise en œuvre de mesures de blocage à l'initiative des pouvoirs publics **(§2).**

[215] RIVERO Jean MOUTOUH Hugues, *Libertés publiques,* Tome II, 7ème éd. Paris : P.U.F Droit, 2003, (Thémis droit public) n°99, p.102

[216] BIOY Xavier, *Droits fondamentaux et libertés publiques* ,3ème édition (2014), LGDJ Lextenso éditions : Issy-les-Moulineaux, 2014, (Collection cours, dirigée par Bernard Beignier), n°1243, p.539.

[217] MORANGE Jean, *Manuel des droits de l'homme et des libertés publiques,* Paris : P.U.F. Droit, 2007 (Manuels, Collection droit fondamental dirigée par Stéphane Rials), n°96, p.144.

[218] Sur l'impossible multiplication des délits de consultation, v. *infra* « Chapitre 2ème : « La règlementation des limitations à certains sites et services».

§1) La sélection nécessairement autoritaire des sites accessibles à l'internaute

98. ***Plan.*** L'évolution de la structure du réseau de plus en plus centralisée permet aux régimes autoritaires d'établir un contrôle efficace des connexions **(A)** qui peuvent être limitées aux seuls points situés à l'intérieur du territoire national comme cela est le cas en Chine **(B).**

A] La centralisation croissante de la structure du réseau

99. **La centralisation des communications via des serveurs de données**. Il convient d'appréhender le rapport du réseau à l'espace, c'est-à-dire la façon dont les communications sont transmises d'un point à un autre du globe. Alors qu'il s'agit d'organiser la circulation de l'information, le vocabulaire est le même que celui visant le déplacement des personnes. Les paquets de données empruntent différentes passerelles ou ponts[219] ; on dit qu'ils sont routés[220].

Or la structure logicielle[221] du réseau est plus centralisée qu'elle n'y parait, ce qui facilite la visualisation des chemins empruntés et permet dès lors un contrôle. En effet, à l'origine le propre du réseau est d'être décentralisé, c'est-à-dire que chaque ordinateur est dans la chaîne d'acheminement du message, à la fois client et serveur. Un poste informatique, pour utiliser un terme qui renvoie à l'époque des débuts de l'internet, peut à la fois requérir une ressource qui va lui être transmise et stocker cette ressource pour qu'elle puisse atteindre un autre poste. Toutefois l'évolution de la taille du réseau et la diversification des services proposés vont orienter la structure vers une architecture qui oppose les clients aux serveurs[222]. Le réseau est ainsi aujourd'hui constitué de serveurs identifiés, c'est-à-dire des machines à la puissance de calcul importante qui ont pour seul objet de faire tourner des programmes fournissant des services spécifiques[223], que ce soit l'accès à l'annuaire mondial des noms de domaines, à un service de messagerie

---

[219] Voir l'entrée « passerelle (informatique) » sur le site fr.wikipédia.org. « En *informatique, une passerelle (en anglais, gateway) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet.* »

[220] De la même manière que s'opère un routage des journaux, autrement dit une livraison obéissant à un triage de ceux-ci en fonction de leurs lieux de destination, la transmission des données sur le réseau obéit à un schéma de sélection des chemins qui vise l'efficacité de la transmission. V. l'entrée « routage » *in* Dictionnaire Le petit Larousse illustré 2015, et l'entrée «routage» sur le site fr.wikipédia.org.

[221] La structure logicielle du réseau se différencie de la structure physique de celui-ci faite de câbles et de machines de calcul ; elle vise les techniques de transmission du message sur cette dernière.

[222] » FRANCQ Pascal, *Internet, Tome 1 : La construction d'un mythe,* Bruxelles : E.M.E (Editions Modulaires Européennes) (Techno, logos, €Ţ Polis), 2011, p. 65.

[223] « *Un serveur d'Internet n'est rien d'autre qu'un ordinateur sur lequel « tourne » un programme serveur qui exécute la séquence suivante : 1) attendre la requête d'un client, 2) exécuter la requête d'un client 3) envoyer la réponse au client 4) attendre la requête d'un client. Et cela indéfiniment, c'est-à-dire tant que l'ordinateur est en marche. Ses clients sont les autres ordinateurs d'Internet* », VIRIEUX Françoise (Ingénieur de recherche au CNRS), *Comment marche Internet ?,* Editions le Pommier,(Les petites pommes du savoir), 2004, p.10.

électronique ou un service web tel que celui du réseau social Facebook par exemple ou du moteur de recherche Google.

Alors que les points d'émission d'un service ou d'une ressource peuvent être localisés, un contrôle peut s'opérer. Ainsi un État peut interdire l'accès à certains serveurs à la boucle du réseau qui couvre son territoire[224]. Il met en œuvre des systèmes techniques qui contrôlent les passerelles d'accès à son territoire et qui viennent bloquer non pas les contenus qui ne sont pas analysés mais les adresses IP qui peuvent être celles du serveur d'un service tel *Facebook Twitter* ou *Google.*

100. **L'enjeu de l'accès aux serveurs DNS (*Domain Name System)***. Le contrôle du réseau peut intervenir à une échelle plus importante que le blocage de l'accès à certains serveurs de services.

En effet, il faut rappeler que le principe du réseau internet réside dans un système d'adressage unique qui réalise l'interconnexion de tous les réseaux. C'est l'enjeu de la gouvernance d'internet ; l'ICANN pour« *Internet Corporation for Assigned Names and Number »,* une organisation internationale, organise la répartition des adresses IP et leurs concordances avec les adresses URL donnés aux sites[225]. Or ces tables de concordances qui permettent à la connexion de trouver son chemin se trouvent sur des serveurs identifiés organisant le système des noms de domaine (serveur DNS ou *Domain Name System*)[226].

Ainsi il faut envisager que l'accès à ces serveurs DNS hébergeant les tables de concordance entre les adresses IP allouées et les noms de domaine donnés aux sites web puisse être bloqué. Alors que l'internaute n'a plus accès au référentiel commun qui organise l'adressage des différentes ressources à disposition, il est perdu et n'a plus accès à rien ou au contraire il est arbitrairement orienté vers d'autres ressources. Concrètement, l'opération permet de cantonner les connexions à un sous-réseau défini comme celui d'un État. Cet acte unilatéral, s'il marque une volonté de souveraineté, ne peut s'analyser que comme un enferment de l'individu dans les limites d'un territoire. Il est le fait de régimes autoritaires.

B] La création d'un intranet local, le cas de la Chine

[224] De fait, faisant acte de souveraineté eu égard ici à son territoire, l'Etat avant cela, interdit l'établissement d'un serveur d'un service étranger sur son territoire ce qui faciliterait la vitesse de transmission.

[225] V. : pour le détail des ses fonctions, *infra* n°208 et suiv.

[226] V. VIRIEUX Françoise (Ingénieur de recherche au CNRS), *Comment marche Internet ?*, Editions le Pommier, (Les petites pommes du savoir), 2004, p.13.

101. **La Grande muraille pare-feu de la Chine.** L'exemple connu de tous est le cas de la Chine qui a créé un immense Intranet local. Ce filtrage est connu à l'extérieur de la Chine continentale sous le nom de « *Grande muraille pare-feu de Chine* »[227]. La référence à la Grande muraille est révélatrice de la nature de ce filtrage qui empêche l'accès à des serveurs étrangers, autrement dit, aux nationaux d'aller s'informer ailleurs.

Comme l'expliquent Jack Goldsmith et Tim Wu, tous deux professeurs de droit américains, dans leur ouvrage « *Who controls the Internet ? Illusions of a Borderless World* »[228] cette barrière a été construite par l'entreprise américaine Cisco selon le même procédé qui a permis aux entreprises américaines de permettre un accès au réseau à leurs employés sur leur lieu de travail tout en limitant les sites accessibles ; le principe du contrôle des points d'accès des flux d'informations est le même sauf que la population visée est ici celle d'un État. En se dotant de routeurs Cisco, la Chine contrôle les points d'entrée sur son réseau local comme le ferait un « *checkpoint* »[229].

Par ailleurs, la Chine organise également « *un empoisonnement du DNS* »[230] lorsque certains sites particuliers sont demandés. Les demandes n'aboutissent pas car elles ne trouvent pas l'adresse IP correspondante à la ressource recherchée. Ainsi la logique de ce contrôle n'est pas l'analyse des contenus et leur censure alors que celle-ci ne pourrait se faire qu'à la marge en considération de la masse des informations disponibles ; le contrôle vise un isolement des internautes chinois et une reterritorialisation de la boucle du réseau local[231]. Comme le souligne Reporters sans frontières dans son rapport 2007, la Chine mais aussi la Birmanie ou la Syrie « *tentent de faire du Web un réseau limité aux seuls échanges à l'intérieur du pays* »[232] ; faisant cela ces États opèrent une contrainte sur leur ressortissants qui s'apparente à une violation du principe de la liberté d'aller et venir.

102. **La reconnaissance de la liberté de naviguer par un État de droit**. La liberté de circuler pour un national dans le monde physique vise la possibilité qu'a chacun de circuler sans aucune formalité administrative et sans aucun contrôle à travers le territoire national ; ce

---

[227] V. l'entrée « Grand firewall de Chine » sur le site fr.wikipédia.org

[228] J.GOLDSMITH, T.WU, *Who Controls the Internet, Illusions of a Borderless World,* Oxford University Press, 2006, p. 93.

[229] *Ibid.*

[230] V. l'entrée « Grand firewall de Chine » sur le site fr.wikipédia.org

[231] Ainsi sur l'émancipation de la Chine quant à la gestion des noms de domaine eu égard à l'organisation universelle mise en œuvre par les Américains, un auteur s'exprime en ces termes : « *Cet évènement, passé largement inaperçu, est considérable ; il est comparable, dans l'espace virtuel de l'internet, aux guerres commerciales et coloniales des XVIIe et XVIIIe siècles » V.* GUILLAUD H. « Vers un grand schisme de l'internet ? », *Gouvernance de l'internet,* 2010, p.1, cité par , HUET J. et E. DREYER, *Droit de la communication numérique,* Paris : L.G.D.J. 2011 (Manuel), p.20.

[232] V. : SUPLY Laurent, « Les nouvelles trouvailles de la cyber-censure », article mis en ligne 2 janvier 2008 sur le site *Lefigaro.Fr.* Le rapport 2007 est disponible à cette adresse : http://www.rsf.org/IMG/pdf/rapport_fr_bd-2.pdf

principe a valeur constitutionnelle en France et également reconnu au niveau international[233]. Si le droit de se déplacer librement sur le territoire national semble de nos jours évident certains auteurs rappellent que « *Nos aînés ont connu les ausweiss imposés par l'occupant allemand entre 1940 et 1944 pour passer d'une zone à l'autre du territoire français et nos ancêtres, dans la première moitié du XIXème siècle, l'institution du passeport intérieur c'est-à-dire la nécessité d'une autorisation administrative pour les déplacements de quelque importance. »*[234]. La réalité des « *checkpoint* » mis en place techniquement à l'entrée du sous-réseau local Chinois s'apparente à ce contrôle des déplacements des individus qui sont contraints dans leurs choix de connexions.

Une communication doit pouvoir emprunter l'ensemble des points de la structure du réseau et ne pas faire l'objet d'un contrôle par un État dans le but de la stopper. Un Etat ne peut retenir les connexions de ses ressortissants en agissant sur la structure d'une manière telle qu'est amputée la liberté de naviguer sur celui-ci alors que les choix de connexions sont réduits au réseau local. Il faut différencier en cela la politique des États démocratiques qui cherchent, avant que de contrôler l'individu, à réguler les activités du réseau.

§2) La nécessaire gouvernance des sites mis en ligne sur le réseau

103. **Le rôle de la « puissance » publique**. Comme le soulignent les professeurs Frier et Petit dans leur manuel de droit administratif, citant la doctrine de Duguit visant le rôle de l'État : « *Celui-ci ne saurait plus faire usage de la puissance pour la puissance ; s'il peut intervenir c'est parce qu'il est seul à même de remplir cette mission obligatoire qui a des objectifs tels que « son accomplissement doit être assuré, réglé et contrôlé par les gouvernants, parce que l'accomplissement de cette activité est indispensable à la réalisation et au développement de l'interdépendance sociale, et qu'elle est de telle nature qu'elle ne peut être réalisée complètement que par la force gouvernante* »[235].

Ainsi aux tenants d'un internet libertaire, qui ne voient dans l'action de l'État que la contrainte et la force employées, il convient de rappeler que celle-ci est légitime car nécessaire dans le sens où seul un acte d'autorité peut venir limiter la liberté de tous. La logique est alors de considérer les troubles pouvant se développer sur le réseau en

[233] Comme le soulignent J.Rivero et H. Moutouh, ce principe a valeur constitutionnelle (CC, 12 juillet 1979) et est également consacré comme « liberté fondamentale » par le Tribunal des conflits (TC, 9 juin 1986, *Eucat*), la Cour de cassation (Cass. Civ. 28 novembre 1984, *Bonnet)* et est aussi reconnu sur le plan international : Protocole n°4, art. 2 de la Convention européenne des droits de l'homme, article 12 du Pacte onusien de 1966 sur les droits civils et politiques. V. RIVERO Jean MOUTOUH Hugues, *Libertés publiques, op. cit.,* n°99 p.102. V. pour un détail des sources internationales qui distinguent cette liberté de la liberté individuelle, BIOY Xavier, *Droits fondamentaux et libertés publiques, op. cit.* p.536.

[234] RIVERO Jean MOUTOUH Hugues, *Libertés publiques, op. cit.,* n°99 p.102

[235] FRIER P. L. et J. PETIT, *Droit administratif,* 9ème éd., Issy-les-Moulineaux : LGDJ Lextenso Editions, 2014.

mettant en œuvre une surveillance des activités qui s'y développent **(A),** ce qui permet de fonder le choix d'une mesure administrative qui a pour but de prévenir les troubles à l'ordre public dans l'intérêt de chacun **(B).**

A] Les contours de la surveillance du réseau

104. **Le sens d'une surveillance**. La définition du mot « *surveillance* » qui est : « *l'action de veiller sur une personne ou une chose dans l'intérêt de celle-ci, ou de surveiller une personne ou une opération pour la sauvegarde d'autres intérêts* »[236] fait apparaître que la surveillance du réseau par les pouvoirs régaliens s'opère dans l'intérêt même des individus qui y ont accès. En effet si le réseau n'est pas surveillé et dès lors gouverné, l'État est tenté de mettre en œuvre une surveillance des faits et gestes de l'individu.

Une contrainte sur l'individu qu'il faut condamner et empêcher en restaurant un régime effectif de régulation des activités se développant sur le réseau. C'est le second sens du mot « surveillance » : « *action préventive qui, fondée sur la vigilance de celui qui surveille (marquée par des actes de vérification et de contrôle), s'applique à l'action d'autrui dans le temps (au développement, au devenir de ce qui est surveillé)*»[237]. Or il faut constater que ce régime nécessaire de prévention des troubles à l'ordre public n'est pas reconnu sur le réseau. Un mouvement sclérosant s'opère alors qui tend à réprimer pénalement l'activité de l'internaute notamment à travers la définition de délits dits de « consultation habituelle » de sites. Or si d'ordinaire le régime répressif est le plus libéral, le dévoiement de sa logique questionne ici les valeurs de l'État de droit. De la même manière qu'on ne peut contraindre la liberté de naviguer d'un individu en sélectionnant un ensemble de sites qui lui sont accessibles, on annihile celle-ci si les troubles à l'ordre public ne sont pas prévenus[238].

105. ***Plan.*** D'une part, l'on s'interrogera ainsi sur l'objet de la surveillance du réseau. Il sera vu que s'il est nécessaire d'associer le FAI à la détection des comportements s'y développant, la surveillance de la mise en ligne de certains contenus sur le web relève en revanche des hébergeurs **(1)**. D'autre part, il faut questionner l'objectif de cette surveillance. Il sera vu que la surveillance doit viser la sauvegarde de l'ordre public et non la répression des infractions de communication **(2)**.

---

[236] V. : l'entrée « surveillance » *in* CORNU G., *Vocabulaire juridique*, 10ème éd., Paris : P.U.F, 2014.

[237] *Ibid.*

[238] Il est à noter que dans la même logique d'un rapport d'autorité, le titulaire de l'abonnement d'un point de connexion au réseau peut filtrer les sites accessibles à partir de son point d'accès. La logique n'est pas d'en faire le responsable des usages fait de celui-ci mais de considérer que ce filtrage relève de son pouvoir de limiter les déplacements sur le réseau des personnes à qui il met à disposition l'accès, ainsi d'un parent vis-à-vis de son enfant ou d'un employeur vis-à-vis de son salarié.

1) L'objet de la surveillance : les flux de communications visualisés par le FAI et non les contenus mis en ligne via un hébergeur

106. **Le FAI, acteur privilégié de la surveillance du réseau**. L'activité du FAI le place comme l'acteur pouvant apprécier la nature des flux de connexions et les points vers lesquels ils sont acheminés.

Ainsi il peut considérer les sites web les plus demandés et ainsi opérer une cartographie des usages de la structure du réseau, cartographie qui peut renseigner les pouvoirs publics sur l'utilisation de celui-ci et l'émergence de nouvelles pratiques qui peuvent consister en des activités illicites ou des troubles à l'ordre public. Il peut également par exemple considérer que la bande passante est largement utilisée pour télécharger des fichiers lourds tels que des fichiers audiovisuels par exemple et faire état auprès des autorités de la nature du service ou du nom du site qui opère une telle activité ; ainsi de l'usage d'un réseau P2P ou d'un site de streaming, ce qui toutefois ne présage en rien de la nature des fichiers téléchargés.

L'objet est ici la surveillance du réseau et des activités qui s'y développent. Il ne s'agit pas de suivre une connexion spécifique et de considérer les allers-et-venus d'un individu. Il ne s'agit pas non plus de surveiller le web et de considérer l'ensemble des propos qui s'y tiennent[239]**.** La surveillance n'a de sens qu'eu égard au développement d'une activité et non s'agissant de la mise au jour d'une infraction de communication nécessairement publique. Or maladroitement la législation établit un régime commun aux FAI et aux hébergeurs de contenus mis en ligne sur le web s'agissant de leur obligation de lutte contre les infractions réalisées sur le réseau.

107. L**a malfaçon législative du rapprochement des régimes du FAI et de l'hébergeur s'agissant de la lutte contre les infractions se réalisant sur le réseau : l'article 6-I-7 de la LCEN.** L'article 6-I-7 de la Loi pour la Confiance en l'Economie Numérique[240] (LCEN) énonce dans un premier alinéa que les personnes mentionnées aux 1 et 2, c'est-à-dire d'une part les FAI et d'autre part les hébergeurs de contenus, « *ne sont pas soumises à une*

[239] La formulation adoptée fait ici volontairement référence à la mise en relation d'individus et non à la mise en ligne de contenus.

[240] Loi n°2004-575 du 21 juin 2004 « *pour la Confiance en l'économie numérique* », JORF du 22 juin 2004, Texte 2 sur 108.

Voir de la même manière, le champ d'application de l'article 15 « *Absence d'obligation générale en matière de surveillance* » de la directive de 2000 dite « *commerce électronique* » qui vise non seulement les prestataires de simple transport, que sont les FAI, mais également les prestataires de stockage automatique dit de « *caching* », et les prestataires d'hébergement. Directive 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, JOCE L178/1-16.

obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou circonstances révélant des activités illicites ».

La lecture de ce premier alinéa fait apparaître qu'une différenciation devrait être faite entre la surveillance des contenus transmis et stockés et la détection des faits et activités illicites. Les régimes visant l'activité des FAI et celle des hébergeurs qui s'entrecroisent dans la longue rédaction de l'article 6 de la LCEN gagneraient à être dissociés.

En effet, aujourd'hui, alors que les problématiques ne sont plus celles du web 2.0 qui voyait l'émergence de la prise de parole de tout à chacun, une distinction apparaît quant à leurs obligations respectives. Le mérite de la LCEN et de son article 6 est d'avoir établi en 2004 un régime de régulation des contenus mis en ligne dès lors qu'ont été aménagées les responsabilités civile et pénale de l'hébergeur. Le système de retrait après une notification prévu par l'article 6. I. 2 et 3, qui doit répondre de certains critères[241] est effectif et permet de désengager les hébergeurs de toute surveillance quand à la tenue de propos illicites. Une régulation des contenus s'opère en deux temps : elle peut d'abord être mise en œuvre par l'hébergeur notifié, elle ressort *in fine* du juge judiciaire, seul compétent, si un contentieux apparaît, pour opérer la balance des intérêts en présence alors qu'est en jeu la liberté d'expression.

Cette procédure étant détaillée à l'article 6-I de la LCEN, aux points 2,3, et 5, le point 7 organise en réalité, parallèlement à ce régime de responsabilité aménagée[242], la surveillance de certains contenus spécifiés, qui se conçoit à l'égard des hébergeurs mais est peu lisible s'agissant de l'activité des FAI.

2) L'objectif de la surveillance : la détection des troubles à l'ordre public et non la dénonciation des infractions de communication

108. **L'ineffectivité pour les FAI de la mention des infractions de communication et de leur dénonciation dans un standard ouvert**. L'alinéa 3 de l'article 6-I-7 de la LCEN énonce

[241] Article 6.I.5 de la LCEN.

[242] Le régime de la mise en œuvre de la responsabilité après notification à l'hébergeur par un tiers d'un contenu manifestement illicite doit selon nous être dissocié de la régulation s'agissant de la mise en ligne de contenus réalisant des infractions spécifiées par le législateur.

La problématique n'est pas celle de la responsabilité pénale des hébergeurs alors que avertis, par un message déposé dans un standard ouvert, ils sont d'abord tenus, au tire de l'article 6.I.7 al.3, d'en informer les autorités publiques compétentes ; l'auteur de l'infraction doit être poursuivi, le retrait du contenu ne doit intervenir que dans un second temps. L'hébergeur peut être sanctionné pénalement au titre de l'article 6.I.7 al. 7 s'il n'a pas mis à disposition ce standard ouvert.

De fait on peut s'interroger, mais il nous semble à la marge, sur les conditions de l'engagement de la responsabilité pénale de l'hébergeur, si informé par des messages répétés dans ce standard ouvert, il avait manqué de diligences. V. DREYER E., « Le blocage de l'accès aux sites terroristes ou pédopornographiques », *JCP G*, n°14, 6 avril 2015, p.685.

que *« Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de la provocation à la commission d'actes de terrorisme et de leur apologie, de l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap ainsi que de la pornographie enfantine, de l'incitation à la violence, notamment l'incitation aux violences sexuelles et sexistes, ainsi que des atteintes à la dignité humaine, les personnes mentionnées ci-dessus doivent concourir à la lutte contre la diffusion des infractions visées aux cinquième, septième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et aux articles 222-33, 225-4-1, 225-5, 225-6, 227-23 et 227-24 et 421-2-5 du code pénal».*

Or en ce qu'il vise des infractions de presse et des infractions de communication qui relèvent de l'appréciation d''un contenu, il apparaît ineffectif de mettre la surveillance de telles infractions à la charge des FAI nationaux. Cette détection ne concerne que les hébergeurs. La première obligation énoncée à l'alinéa 4 de l'article 6-I-7, qui entend que soit mis en place « *un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données »*, ne peut viser qu'un standard ouvert apparaissant nécessairement sur un site du web[243] et mis en œuvre donc par l'hébergeur et non par le FAI. La surveillance des sites mis en ligne et des activités se développant sur le web en général, doit intervenir à un autre niveau : les services de l'État mettent en œuvre des sites dédiés au signalement de contenus ou de sites illicites par les citoyens[244].

109. **L'efficacité de la détection par les FAI s'agissant des activités illicites et leur rôle dans la mise en œuvre de politique de lutte contre celles-ci**. Le second alinéa de l'article 6-1-7 de la LCEN énonce que peut être mise en œuvre *« une activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire* ». Celle-ci ne peut logiquement viser à l'inverse que les FAI et la surveillance proactive de certains flux de connexion, alors que la surveillance du contenu mis en ligne, disponible aux yeux de tous, ne requiert pas de procédure particulière. Mais de fait il faut souligner qu'alors que la cartographie des flux de connexions ne révèle pas d'informations personnelles sur les individus à l'origine des connexions, la mention du juge judiciaire apparaît inutile.

La détection des activités illicites se réalisant sur le réseau n'a pas à être mise en œuvre par le juge judiciaire ; la logique de la surveillance du développement de la criminalité n'est pas celle de la surveillance d'un individu. Elle répond de politiques

[243] Alors qu'on voit mal comment un FAI pourrait mettre en œuvre un tel standard.
[244] V. La plateforme dite « Pharos » : www.internet-signalement.gouv.fr

publiques qui viennent viser des activités spécifiques. L'alinéa 5 de cet article 6-I-7 cite seulement l'intérêt général attaché à la *« répression des activités illégales de jeux d'argent* ». Il faudrait donner davantage corps à une politique de lutte contre la criminalité organisée sur le réseau qui englobe notamment la mise en œuvre de réseaux pédopornographiques ou de réseaux à visée de propagande et de recrutement pour le Djihad, politique criminelle dont il faut considérer qu'elle ne vise pas dans un premier temps la sanction des criminels qui mettent en œuvre ces réseaux mais la protection de l'ordre public et des administrés.

La seconde obligation de l'alinéa 4 de l'article 6-I-7 énonce s'agissant tout à la fois des hébergeurs et des FAI : « *elles ont également l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activité illicites* ». Cette obligation renvoie à la nécessité de poursuivre un individu à l'origine d'un contenu réalisant une infraction visée par l'alinéa 3 et signalée à l'hébergeur. En revanche il est difficile d'envisager les contours de cette obligation à l'égard de flux de connexions et d'activités illicites si celles-ci ne sont pas davantage spécifiées alors qu'un FAI ne peut agir que sur un site en son entier via le blocage de son accès. A cet endroit, un État dit de droit, doit définir la réalité des troubles à l'ordre public pour fonder les mesures prises qui doivent être nécessairement rendues publiques et obéir à un régime strict de mise en œuvre.

B] La nature administrative des mesures à mettre en œuvre

110. **Une mesure d'ordre public mettant en œuvre le service public de l'accès au réseau**. La demande de blocage d'un site ne peut se faire à l'initiative des particuliers quand bien même la mesure est décidée par le juge judiciaire. Toute action en justice en ce sens auprès d'un FAI s'oppose à la liberté de navigation qui doit être garantie à tout internaute, principe qui n'est pas un blanc-seing à la diffusion de tout contenu mais qui renvoie à la mise en œuvre d'un régime de liberté publique.

Or il faut constater le recours systématique à la procédure de référé, quelque soit son fondement,- l'article 809 alinéa 1er pour le droit commun, ou les articles 6-I-8 de la LCEN ou L336-2 du CPI pour les référés spéciaux[245]-, en vue de bloquer un site du web.

[245] Pour une application combinées des articles 809 al 1 CPC et 6-I-8 LCEN : v. CA Paris, pôle 1, ch. 2, 28 mai 2015 pour un cas de trouble de concurrence déloyale du fait du non respect d'un réseau de distribution sélective, -M. MALAURIE-VIGNAL, *Contrats Concurrence Consommation,* 2015, comm. 227-. Pour une application de l'article 336-2 CPI : v. l'affaire dite « Allostreaming » du nom d'un des sites tendant à être bloqué, CA Paris, pôle 5, chambre 1, arrêt du 15 mars 2016, confirmant sauf sur la charge des coûts de blocage qu'elle fait peser sur le FAI, l'ordonnance de référé du TGI de Paris, du 28 novembre

Dans une étude intitulée « Vers un référé de l'Internet autonome », Béatrice Gorchs dénonce cette « *procéduralisation du droit par la voie du référé* » et souligne pour conclure sa démonstration que : « *C'est peut être dans les référés Internet que gît l'avenir du référé, une justice rapide mais qui en définitive, devient parallèle à la justice ordinaire, un instrument de police efficace mais qui, provisoire émancipe le juge des fondements civilistes de notre droit »*[246]. Or non seulement une telle instance méconnait les fondements civilistes, en ce que la recherche de la responsabilité de l'auteur du trouble est absorbée par celle de l'efficacité de sa cessation, mais elle méconnait également la liberté fondamentale de naviguer sur le réseau pour l'individu alors que la mesure de police de blocage d'un site doit relever nécessairement d'une politique publique obéissant à un régime défini, transparent et contrôlé.

111. ***Plan***. L'injonction faite par le juge judiciaire aux FAI de bloquer un site n'a pas de sens **(1)** dès lors que seule une mesure d'administration publique pérennise ce blocage efficacement **(2).**

1) Le non-sens de la mise en cause des FAI devant le juge judiciaire

112. **Le dévoiement de la mise en œuvre de la responsabilité du FAI.** Les FAI répondent de la mise en œuvre du service public de l'accès. Ils sont les acteurs privilégiés de la mise en œuvre de la liberté d'accès au réseau et de la liberté de naviguer sur le web.

Toutefois le caractère fondamental de ces libertés n'est pas formellement reconnu dans la législation européenne et française. Dès lors cherchant non plus à organiser le retrait d'un contenu comme à l'heure du web 2.0 mais bien à organiser le blocage d'un site dans le cadre du web applicatif, les juges européens et français viennent très maladroitement questionner, dans la droite ligne de la responsabilité aménagée des

---

2013, *APC et al c/ Auchan télécom et al.*- O. PIGNATARI, *RLDI* 2013/99, n°3293. V. également l'affaire « The Pirate Bay » : TGI Paris, 3ème ch. réf., 4 déc. 2014, -L. GRYNBAUM, *RLDI* 2015, actu112. Pour une application de l'article 6-I-8 LCEN : v. l'affaire « Aaargh » du nom de l'Association des Anciens Amateurs de Récits de Guerre et d'Holocauste, qui émettait des propos négationnistes sur un site, Cass. 1ère civ. 19 juin 2008, n°07-12244, *Bull.,* 2008, I., n°178, et l'ordonnance de référé du TGI de Paris du 13 juin 2005, disponible sur le site legalis.com, -C. HUGON, *JCP G* 2008, n°42 II 10171, C. CARON, *CCE* 2008, comm.99, Ph. STOFFEL-MUCNK, *CCE* 2005, comm. 140.

Il est intéressant de noter l'évolution des contentieux alors que la mesure de blocage s'est déplacée de la sanction d'une infraction de communication à la lutte contre la contrefaçon, et qu'elle est en 2015 pour la 1ère fois appliquée pour sanctionner les règles de la concurrence déloyale. La mention de l'article 809 al. 1er semble alors requise comme si l'article 6-I-8 de la LCEN apparaissait trop spécialisé eu égard au contentieux de la mise en ligne de propos sur le Web 2.0 qui l'a vu naître.

[246] GORCHS Béatrice, «Vers un référé de l'Internet autonome », *CCE* 2007, étude 31. *Contra,* mais dès lors selon une position que nous condamnons, Sophie HOQUET –BERG à propos de l'injonction faite en référé aux FAI de bloquer le site « Aaargh » énonce pour sa part : « *Cette décision nous paraît devoir être approuvée car elle sacrifie à l'efficacité et au pragmatisme, un juridisme sclérosant* », HOQUET-BERG S., « Pouvoirs du juge des référés à l'égard des fournisseurs d'accès à l'internet », note sous Cass. 1ère. Civ.,19 juin 2008 *op.cit., Resp. civ. Assur.,* 2008, comm. 256.

hébergeurs, les contours d'une responsabilité des FAI eu égard à l'accès à certains sites du web.

En effet même s'il est patent que le FAI ne peut être responsable des activités de l'ensemble des sites de la toile et que de fait il n'est soumis à aucune obligation générale de surveillance à cet endroit, les décisions visent le FAI puisqu'il est le seul acteur à même de prendre une mesure techniquement efficace. Dès lors les raisonnements apparaissent forcément spécieux.

Ainsi le juge européen qui considère que le contrôle des flux dans le cas d'un réseau P2P apparaît trop général mais valide que soient bloqués des sites de streaming spécifiés[247], ne peut mener le raisonnement à son terme dès lors que pour ménager la liberté d'entreprendre des FAI qui sera d'autant amputée que les coûts de ces mesures seront importants et que celles-ci se multiplieront, indique que « *le destinataire d'une telle injonction a la possibilité de s'exonérer de sa responsabilité et ainsi de ne pas adopter certaines mesures éventuellement réalisables, dès lors qu'elles ne sont pas susceptibles d'être qualifiées de raisonnables* »[248]. Comme le souligne alors le professeur Caron : « *comment admettre que le destinataire d'une décision de justice puisse, de sa propre initiative, décider de ne pas l'exécuter au prétexte qu'elle serait déraisonnable* »[249]. Le choix de la mesure doit ressortir d'une limitation et d'un contrôle objectifs.

113. **Le dévoiement de la procédure de référé.** L'étude des instances introduites devant le juge des référés français pour bloquer un site fait apparaître que d'une part cette procédure n'enjoint plus à une mesure provisoire et que d'autre part en opérant un contradictoire qui n'a pas lieu d'être elle se révèle inefficace.

Ainsi en effet il apparaît d'une part clairement que le but de telles instances n'est plus de faire cesser le trouble de manière provisoire dans l'attente d'un jugement au fond mais bien de réaliser la cessation du trouble. Le blocage du site se confond en effet

[247] V. CJUE 24 novembre 2011, aff. C-70/10 *Scarlet Extended Sa c/ SABAM*, portant sur une demande de mise en place de filtrage des communications électroniques, et CJUE 27 mars 2014, aff. C-314/12 *UPC Telekabel Wien c/ Constantin Film Verleih Gmbh*, portant sur des sites internet mettant des œuvres cinématographiques à la disposition du public sans le consentement des titulaires d'un droit d'auteur ou voisin. Pour un panorama v. *D.* 2014 n°440, p.2326

Dans le même sens, en droit interne, le juge français qui énonce que « *Cependant les mesures sollicitées sont spécifiques aux sites visés par les demandeurs et le flux des communications concernées ne représentent qu'une part infime de l'activité des FAI laquelle ne peut être affectée qu'à la marge* », v. TGI de Paris, du 28 novembre 2013, *APC et al c/ Auchan télécom et al.*, disponible sur le site legalis.net

L'on peut apprécier la distinction faite dans cette étude entre la condamnation de tout filtrage étatique et le nécessaire régime de mesures administratives de blocage.

[248] CJUE 27 mars 2014, aff. C-314/12 *UPC Telekabel Wien c/ Constantin Film Verleih Gmbh*, point n°59.

[249] CARON C., « Le blocage de sites contrefaisants une nouvelle fois devant la Cour de justice de l'Union européenne », *CCE*, 2014, comm. 43.

avec l'effet recherché de l'action au fond qui devrait viser le site en ligne et sa fermeture, mais qui dès lors n'a plus lieu d'être. Alors qu'il est difficile de fermer un site souvent basé à l'étranger, la voie des référés se suffit à elle-même [250] à première vue.

A première vue seulement, car il apparait en effet que le blocage d'un site est inefficace à réaliser la sanction pénale qui est recherchée dès lors que si le créateur du site n'est pas inquiété pour la mise en ligne de celui-ci, la fonction « *intimidatrice* »[251] de cette sanction n'est pas atteinte. Or ce seul objectif est efficient dans le cas de la mise en ligne d'un site alors qu'un nouveau site peut être ouvert si l'auteur même n'a pas été sanctionné. Il en va de même pour le blocage relatif à d'autres contentieux tel celui des sites de streaming, ou ceux opérant une concurrence déloyale en méconnaissance des règles de distribution sélective qui peuvent déplacer leur activité par le truchement d'un nouveau nom de domaine[252].

D'autre part, la problématique du coût des mesures de blocage fait apparaître l'inadéquation de la mise en cause des FAI dès lors que ce ne peut être à eux de supporter financièrement la sanction des actions illicites qui ont lieu sur le réseau. On le voit le blocage d'un site doit bien relever d'une injonction de faire mais qui doit se réaliser dans une mesure d'administration publique.

2) L'efficacité d'une mesure administrative à leur encontre

114. **La problématique de l'actualisation de la mesure**. La limite d'une action en référé apparaît concernant l'actualisation de la mesure. Le juge déclare son incompétence à « *contrôler l'exécution de sa décision, soit directement soit par l'intermédiaire d'un agent public qui en aurait la charge* »[253]. Il mentionne un accord possible entre les parties dans le cadre du suivi des mesures et souligne même que : « *l'ensemble des FAI, à l'exception de Free, avait accédé aux demandes des titulaires de droit sans décision judiciaire et pris des mesures techniques empêchant le téléchargement de fichiers lourds* »[254]. Or une telle

[250] V. sur cette « *évolution de certaines procédures de référé vers des procédures autosuffisantes*», GORCHS Béatrice, *op. cit.*

[251] PRADEL Jean, *Droit pénal Général*, Editions Cujas, 17ème éd. Paris : 2008-2009, n°563.

[252] Même si toutefois à cet endroit à la différence d'une page ou d'un site permettant l'expression en ligne et mis en œuvre via une plateforme d'hébergement, la procédure de changement de nom de domaine peut s'avérer si ce n'est plus problématique à tout le moins plus longue. Ainsi il est à noter que le site bloqué en tant que www.alloshowtv.com en 2013 est à nouveau accessible en mai 2016 sous le nouveau nom de domaine www.allo-show.tv.com (une syntaxe différente pour l'enregistrement du nom mais qui évidemment n'a pas d'incidence sur la recherche effectuée pour trouver ce site via un moteur de recherche).

[253] TGI de Paris, du 28 novembre 2013, *APC et al c/ Auchan télécom et al.*,

[254] *Ibid.* Il est à noter que seule la société Free parmi les FAI appelés en la cause a argué qu'elle ne pouvait le faire qu'après ordonnance du juge judiciaire.

argumentation qui méconnait la liberté de naviguer sur le réseau ne peut être entendue. La mention du recours à « *un agent public* » témoigne de la nécessité d'une actualisation décidée unilatéralement. On le voit la mise en œuvre d'une mesure de blocage doit être à l'initiative des pouvoirs publics.

115. **La problématique des coûts de blocage.** Cette nécessité apparaît également à l'endroit de la prise en charge des coûts des mesures de blocage. La jurisprudence se divise actuellement ne sachant pas s'il faut faire peser ceux-ci sur les demandeurs à l'action qui arguent du respect de leurs droits[255] ou sur les FAI[256] ; et de fait, ils n'ont à être pris en charge ni par l'un, ni par l'autre.

Ils doivent être pris en charge par l'État dans le cadre d'une politique publique qu'il souhaite mettre en œuvre et dont les contours sont définis, ce qui limite le recours à une telle mesure qui ne peut être la solution de la sanction de toutes les infractions commises sur le réseau.

Section II. La régime d'une mesure de police administrative spéciale

116. **Le régime d'une liberté publique**. L'analogie avec la liberté d'aller et venir permet d'appréhender la nécessité d'un acte d'autorité et ses limites.

En effet, la souveraineté de l'État est fondée par son rôle de sauvegarde de l'ordre public. Or si les pouvoirs publics ne peuvent sur ce fondement en dehors de toute procédure judiciaire couper l'accès d'un individu au réseau, leur action est en revanche nécessaire et la seule légitime pour mettre en œuvre le blocage de certains points de connexion pour assurer cette mission auprès de leurs administrés. Ainsi, il faut souligner que toute demande de blocage à l'initiative d'un particulier ne peut aboutir dès lors que la délimitation des sites accessibles ne peut ressortir des administrés eux-mêmes.

Le blocage de sites participe du régime de la liberté de navigation et ne réalise pas une atteinte à celle-ci tant que l'action de l'administration ne porte pas sur les connexions des internautes qui ne sont visées que si le blocage est généralisé et arbitraire ce qui ampute alors d'autant leur liberté de choix. Ainsi l'action de l'administration répond en l'espèce d'un régime éprouvé : celui de la défense d'une liberté publique.

[255] TGI Paris, réf., 28 nov. 2013 *APC et al c/ Auchan et al* (Affaire « Allostreaming »), et TGI Paris, 3ème ch., 1ère section, 4déc. 2014, (Jugement « The Pirate Bay »), disponibles sur légalis.net

[256] En ce sens récemment, v. : CA Paris, Pôle 5, chambre 1, 15 mars 2016. La Cour d'appel, dans l'affaire « Allostreaming », s'oppose au TGI sur ce point. V. : LE GOFFIC Caroline, « Décision Allostreaming : légalité des mesures de déréférencement et coût de blocage à la charge des intermédiaires techniques », *Dalloz IP/IT* 2016, 372.

117. ***Plan***. Les conditions du blocage doivent être prévues par la loi. L'action nécessaire de l'administration est donc enserrée dans les limites de l'objet d'une police administrative spéciale **(§1)**. Le contrôle de la mise en œuvre d'une telle mesure apparaît ainsi à deux niveaux : le contrôle constitutionnel de l'étendue de la loi d'habilitation et le contrôle administratif de la mise en œuvre du contenu de celle-ci **(§2)**.

§1) L'objet de la police administrative spéciale dotée d'une telle mesure

118. **La sanction administrative d'une activité illégale ou troublant l'ordre public et non la sanction pénale d'un contenu illicite**. Alors que le blocage d'un site le vise en son entier, il convient de considérer que l'illicite ne peut se constater que s'agissant d'un site offrant un service qui porte atteinte à l'ordre public, ou un site web ou une page internet dont le contenu envisagé de manière générale[257] réalise cette même atteinte. Le blocage vise techniquement une adresse URL. Ainsi la mesure de blocage ne peut renvoyer à un contenu spécifié comme un commentaire ou une image dont la sanction doit être envisagée sur le terrain du droit de la communication. Il a été vu qu'est organisé un système de détection de contenus réalisant des infractions spécialement visées et qu'une procédure de retrait après notification est établie par la LCEN. Un service proposant un hébergement de contenus doit retirer une page réalisant une telle infraction, comme un profil facebook ou un article de blog et permettre par ailleurs l'identification de son auteur.

Le fait que la mise en œuvre de cette régulation « *butte sur les données factuelles* » pour reprendre l'expression d'un commentateur dans l'affaire « Aargh »[258] qui dans le cas de propos négationnistes voyait le juge français démuni face à des hébergeurs américains qui assignés à parquet étranger n'avaient pas comparu, ne doit pas conduire à la conclusion de son inefficacité[259]. Le mécanisme établi par la LCEN

---

[257] Ainsi Alexandre Linden, « *la personnalité qualifiée prévue par l'article 6-1 de la loi n°2004-575 créée par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme* » indique dans son Rapport d'activité 2015 qu'une recommandation a été prise concernant une photographie de personnes décédées gisant au sol prise à l'intérieur du Bataclan, qui a été publiée sur des réseaux sociaux, des blogs et un organe de presse généraliste suisse. Il rappelle que, alors que l'OCLCTIC souhaitait faire retirer cette photographie diffusée massivement, «*la possibilité de demander le retrait ou le blocage d'un contenu diffusé en ligne, telle qu'elle est prévue à l'article 6-1 de la loi du 21 juin 2004, suppose que le contenu soit en tant que tel constitutif du délit de provocation à des actes de terrorisme ou d'apologie de tels actes. En conséquence seul le contexte de la diffusion de cette photographie était de nature à caractériser ces infractions. Dans le cas d'espèce, il a été estimé que tel n'était pas le cas pour 96 des URL dont le retrait était demandé par l'Office, la photographie en cause faisant l'objet soit d'un traitement neutre, soit d'une dénonciation explicite des actes de terrorisme commis* », Rapport disponible sur le site de la CNIL, cnil.fr, « Bilan de la première année de contrôle », p. 13.

[258] Cass. 1ère civ., 19 juin 2008, n° 07-12244, Assoc . des fournisseurs d'accès et de services Internet (AFA) et a. c/ Assoc. Union des étudiants juifs de France (UEJF) et al., Bull. 2008, I, N° 178. V. C. HUGON, *JCP G* 2008, n°42 II 10171.

[259] Il est intéressant de noter que cette affaire reste la seule à ce jour à avoir fait usage de la procédure de référé de l'article 6-I-8 dans le cas d'un délit de communication prévu par la loi sur la presse (article 24 *bis* de la loi du 29 juillet 1881). Elle s'inscrit dans la droite ligne de l'affaire *Yahoo Auctions (*TGI Paris, ord. réf. 22 mai 2000, *Association « Unions des*

dans la droite ligne de la responsabilité en cascade du droit de la presse doit s'étudier à l'échelle de l'ensemble du contentieux des contenus mis en ligne sur le réseau. Ce mécanisme de détection de contenus spécifiés et de retrait après notification de contenus manifestement illicite est pragmatique alors que par ailleurs les hébergeurs peuvent être enjoints de faire cesser le trouble[260] ; en revanche il faut insister sur le fait que la mise en œuvre d'un blocage à l'échelle des FAI pour sanctionner un délit de communication ne l'est en aucun cas[261]. Au contraire, une telle mesure apparait non pas pragmatique, mais arbitraire en ce qu'elle fige la répression dans une mesure unilatérale qui au-delà de son inefficacité totale, annihile toute réflexion autour d'une régulation à l'échelle internationale de la liberté d'expression alors que la délimitation d'un régime de police à cet endroit ne peut être[262].

119. **Des régimes de polices administratives spéciales.** Il convient d'utiliser le pluriel et de considérer l'épanouissement de plusieurs régimes de polices administratives spéciales. En effet si l'on peut être tenté dans un premier temps de définir la spécialité de la police en charge du maintien de l'ordre public sur le web en considération du support qu'elle vise, le réseau de communication qu'est internet, -elle s'apparenterait ainsi à la police administrative spéciale visant les œuvres cinématographiques[263] -, il faut s'en garder ; car ce serait réduire la

---

étudiants juifs de France », la « Ligue contre le racisme et l'antisémitisme » c/ Yahoo ! Inc. et Yahoo France, disponible sur le site legalis.net), alors que l'association émettant des propos négationnistes avait opéré des délocalisations successives de son site vers *in fine* un hébergeur américain. De la même manière, dans l'affaire Yahoo l'entreprise américaine était attraite devant les tribunaux français pour la mise en ligne d'objets nazis sur son site américain, site qui était accessible au public français. Si à cette époque, l'injonction consistait pour le site américain à bloquer l'accès de ces pages à l'audience française, la logique de la mesure de blocage du site imposée aux FAI français est la même. Il faut contraindre un public ce qui ne peut être. De la même manière que l'on ne peut imposer à une entreprise de filtrer ses contenus suivant l'ensemble des législations nationales, les FAI ne peuvent bloquer l'ensemble des sites mondiaux qui contreviennent à la législation française en matière de liberté d'expression.

La réflexion doit s'extraire du contentieux du droit de la presse et des délits de communication, et du contentieux de la lutte contre la contrefaçon, qui doivent faire face aux deux nouvelles révolutions de l'Internet : la mise à disposition de tous d'un support de publication et la mise à disposition de chacun d'un moyen d'échanges d'œuvres à l'international.

[260] Sur le fondement de l'article 6-I-8 de la LCEN.

[261] V. ainsi la position de la CEDH dans une affaire qui voyait la Turquie attraite devant elle pour le blocage en son entier du service « Google sites », une plate-forme qui hébergeait plusieurs sites Web. Dans le cadre d'une mesure préventive adoptée dans le cadre d'une procédure pénale visant le propriétaire d'un site faisant outrage à la mémoire d'Atatürk, la Présidence de la télécommunication et de l'informatique (PTI) avait en effet bloqué l'accès à la plate-forme en son entier, jugeant que cela était le seul moyen de bloquer l'accès au site, son propriétaire résidant à l'étranger. A juste titre, la CEDH ne se fonde pas sur une appréciation de la proportionnalité de l'atteinte à la liberté d'expression mais condamne sur le défaut de base légale de la mesure. CEDH, 18 déc. 2012, n°3111/10, *Ahmet Yildrim c/ Turquie*, v. : DEBET A., « Blocage de "Google site" : la Cour européenne des droits de l'homme condamne la Turquie », *CCE*, juillet 2013, comm.77.

[262] En ce sens nous souscrivons à l'approche du professeur Emmanuel Dreyer qui énonce que « *la réaction sociale à l'égard des infractions les plus graves* » ne peut être « *un droit administratif prédictif* » qui « *tend à doubler le droit pénal par nature répressive* ». Toutefois nous nous éloignons du raisonnement tenu dans son article intitulé « Le blocage de l'accès aux sites terroristes ou pédopornographiques » en ce que nous soulignons, pour notre part, que la mesure de blocage vise un nom de domaine ou une URL, et donc un site Web ou une page de celui-ci en son entier et non un contenu mis en ligne. V. DREYER E., « Le blocage de l'accès aux sites terroristes ou pédopornographiques », *JCP G*, n°14, 6 avril 2015, p.685.

[263] Qui consiste à délivrer des visas d'exploitation à des œuvres cinématographiques et est attribuée au ministre chargé de la culture par l'article 19 du Code de l'industrie cinématographique.

encore le réseau à son application web, et restreindre cette police aux seules mises en ligne de contenus alors pourtant que le web est de plus en plus applicatif. Envisagé comme un nouvel espace à réguler, la distinction entre différentes polices spéciales apparaît.

L'on peut dès lors s'interroger sur la pertinence d'un régime de contrôle des publications sur le web comme en son temps le régime des publications étrangères[264]. Toutefois, il apparaît que le critère de l'extranéité n'est plus pertinent et qu'alors l'ordre public spécial pouvant venir limiter la liberté d'expression apparaît difficile à délimiter. On ne peut fonder les pouvoirs publics à venir bloquer des sites s'agissant de l'ensemble des infractions de communication.

En revanche, si l'on considère l'ensemble des activités permises par le web applicatif, la délimitation de polices spéciales apparait dès lors qu'elles peuvent venir sanctionner un service défini comme illégal ou un site qui par sa mise en ligne même trouble l'ordre public. Les deux sens que peut prendre la police administrative spéciale peuvent être soulignés. Elle vise d'abord « *des activités de police dont les buts ne sont pas différents de ceux que poursuit la police générale mais qui sont soumis à un régime juridique particulier »*, elle peut encadrer ensuite « *des objets qui ne figurent pas dans le contenu normal de la police générale »*[265], comme la police de l'esthétique, de la chasse ou celle des jeux et loteries.

120. ***Plan***. Une distinction apparaît quant à la fonction de la mesure de blocage : certaines activités peuvent être encadrées spécifiquement et sanctionnées par une mesure de blocage **(A)**. Par ailleurs cette mesure spécifique au réseau peut être envisagée comme un moyen de sauvegarder l'ordre public sur ce nouvel espace **(B).**

A] La sanction d'une activité règlementée

121. ***Plan*.** Le blocage d'un site peut opérer la sanction du non respect de la règlementation séculaire d'une activité comme celle des jeux d'argent et de hasard désormais libéralisés et disponibles en ligne **(1).** En revanche le blocage d'un site dans le cadre de la lutte contre le téléchargement illégal apparait plus problématique alors que la contrefaçon n'est pas réalisée par le site en lui-même ou le réseau de P2P mais par la mise en ligne du contenu **(2)**.

[264] V. Le décret-loi du 6 mai 1939, abrogé par le décret n°2004-1044 du 4 octobre 2004. Pour un historique de ce régime, v. : DREYER E., « Restaurer le contrôle des publications étrangères », *JCP G*, n°40, 4 oct. 2006, I 174.

[265] VEDEL G., DELVOLVE P., *Droit administratif*, 9ème éd., Paris : P.U.F., 1984, (Thémis Droit), p.1062.

1) La sanction de la police des jeux d'argent et de hasard en ligne

122. **Le régime de la loi n°2010-476 « *relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne* »**. Sous la pression de la Commission européenne[266], la France met fin au monopole de la Française des jeux et du PMU et encadre, avec cette loi n°2010-476 « *relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne* », la libéralisation des paris sportifs et hippiques ainsi que celle du poker sur internet[267]. La France fait en l'espèce le choix d'une politique de jeu inédite en Europe alors que l'ouverture à la concurrence est régulée, suivant en cela une longue tradition française en la matière qui ne peut être détachée de la prise en compte de l'historique monopole d'État et donc des enjeux financiers inhérents à l'activité[268].

La loi rappelle toutefois également dans ses articles introductifs, les fondements d'une telle tradition d'encadrement, fondements qui renvoient également à ceux de la politique européenne[269] : la sauvegarde de l'ordre public, de la sécurité publique et la protection de la santé[270] et des mineurs. L'État français exerce en cela ses missions d'autorité de police[271] et est fondé à organiser un régime d'agrément pour les mettre en œuvre. En effet, ce régime en constituant *« une licence ouverte »*[272] se conforme aux exigences européennes de libre-prestation de service et de liberté d'entreprendre. Ce régime est mis en œuvre par une autorité administrative indépendante : l'ARJEL (Autorité de Régulation des Jeux d'Argent En Ligne). C'est elle qui délivre les agréments, les renouvelle, s'assure du maintien de la conformité du service aux conditions de celui-ci et initie le cas échéant une procédure de sanction mise en œuvre par une commission spéciale ou une procédure de blocage du service mise en œuvre par le juge judiciaire.

[266] Une procédure en infraction prévue par l'article 226 du traité CE a en effet été engagée par la Commission européenne en considération de certaines entraves à la libre prestation des services de paris sportifs en France, en Grèce et en Suède. Après avoir examiné les réponses de la France et de la Suède aux lettres de mises en demeure envoyées en avril et octobre 2006, la Commission a officiellement demandé à ces deux pays de modifier leur législation dans le cadre d'avis motivés émis au printemps 2007.

[267] Ne sont pas concernés les jeux et paris réalisés dans les réseaux physiques (loteries et paris hippiques à cet endroit restent du monopole du PMU et de la FDJ). La législation des casinos, implantés physiquement, perdure avec son système d'autorisation. Pour ce qui est des jeux de hasard pur, c'est-à-dire la loterie, l'article 3 II de la loi 2010-476 précise que le monopole d'État perdure.

[268] V. sur les paradoxes de cette libéralisation qui prévoit une autorisation des opérateurs à exploiter ces jeux, et qui régule tout en organisant les revenus fiscaux de cette activité : VILA J.B. « L'ouverture à la concurrence des jeux d'argent et de hasard en ligne : "première étape ou simple palier" d'une régulation ? », *AJDA* 2010 p.1366.

[269] CJCE 6mars 2007, *Placanica*, aff. C-338/04.

[270] Sur la nouveauté toutefois par les pouvoirs publics français de la lutte contre le jeu pathologique, v. : VILA J. B. « Addiction au jeu et santé publique : recomposition de l'ordre public ou nouveau motif d'intérêt général », *AJDA* 2008, p.1804.

[271] VILA J.B., *op. cit.*

[272] VILA J.B., *Op. cit.*

123. **La sanction du non-respect de la procédure d'agrément : le blocage du site par le FAI français**. En effet la loi prévoit dans son article 61 que l'ARJEL adresse à l'opérateur de jeux ou de paris en ligne non autorisé en vertu d'un droit exclusif ou de la procédure de l'agrément prévue à l'article 21, ainsi qu'à toute personne proposant une quelconque offre de jeux d'argent et de hasard en ligne en contravention de la police administrative spéciale visant de tels jeux prévue par le Code de la sécurité intérieure[273], une mise en demeure l'enjoignant à cesser son activité. Si l'opérateur du site n'y a pas fait droit dans un délai de huit jours, le président de l'ARJEL peut saisir le président du TGI de Paris afin que celui-ci fasse ordonner en la forme des référés, l'arrêt de la mise en ligne du service aux hébergeurs, ou le cas échéant le blocage de celui-ci aux FAI. Le décret n°2011-2122 du 30 décembre 2011 visant « les modalités d'arrêt de l'accès à *une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée »*[274] vient définir les conditions de prise en charge des coûts de blocage par l'État.

Si l'on peut questionner le recours au juge judiciaire alors que la loi aurait pu investir l'ARJEL de ce pouvoir de blocage[275], il convient de considérer que cette requête auprès des hébergeurs et à défaut des FAI apparaît tout à fait légitime s'inscrivant dans la logique séculaire de l'encadrement des jeux d'argent et de hasard, activités qui répondent d'une définition et d'un régime clairs. Le pouvoir administratif est fondé à mettre en œuvre le blocage de sites pour transposer celui-ci sur le réseau. En revanche, une problématique à l'endroit de nouvelles activités propres au réseau apparait, services qui permettent la contrefaçon parce que de fait ils sont de nouveaux moyens d'expression en ligne.

---

[273] Titre II « Jeux de hasard, casinos, loteries », du livre III « Polices administratives spéciales » du Code de la Sécurité intérieure.

[274] Décret n° 2011-2122 du 30 décembre 2011 *« relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée* ».

[275] Il faut noter que cette procédure de référé spécial devant le juge judiciaire quand bien même initiée par l'autorité administrative indépendante fait resurgir les mêmes problématiques que les autres demandes en référés visant le blocage de sites. De fait, l'affaire « *StanJames* » (TGI Paris, réf., 6 Août 2010, v. *RLDI* 2010/63, et CA Paris, pôle 1, ch. 3, QPC, 28 juin 2011, v. *RLDI* 2011/74) démontre encore l'inutilité d'un contradictoire avec les FAI. Ainsi dans le cadre de cette instance, un des FAI a introduit une demande de QPC en arguant de la constitutionnalité même de la procédure en cause. Il soutenait que l'article 61 de la loi du 12 mai 2010, en permettant au président de l'ARJEL de solliciter à l'encontre des FAI une injonction de blocage de l'accès à un site Internet sans que l'éditeur du site en cause ait été appelé à la procédure et puisse bénéficier du droit de contester en justice, violait le principe de la présomption d'innocence. La chambre commerciale de la Cour de cassation juge la question non sérieuse en considérant à juste titre que cette procédure et l'injonction qui en découle ne constitue « *ni une peine, ni une sanction ayant le caractère d'une punition, de sorte que ni le principe de la présomption d'innocence, ni le principe du contradictoire ne trouve à s'appliquer à cette procédure qu'institue l'article 61, alinéa 2, de la loi du 12 mai 2010* » (.Cass., com., 18 juin 2013, n°12-28488, v. A. DEBET, *CCE* 2013, comm. 114. V. également Cass. com, 10 déc. 2013, n°12-28488, G. LOISEAU, *CCE* 2014, comm. 17).

La logique d'une mesure de blocage de site non agréé ou illicite en vertu de la police administrative spéciale des jeux répond d'une mesure d'administration nécessaire a l'effectivité du régime imposé et peut être mise en œuvre par l'administration même dès lors qu'elle y est habilitée par la loi.

2) La problématique de la lutte contre les sites de téléchargement illégal

124. **La gageure de la définition d'une activité de diffusion de contenus à encadrer pour lutter contre la contrefaçon**. Alors qu'il est possible qu'une autorité administrative indépendante puisse être investie d'un pouvoir de blocage de sites, il convient toutefois de se garder de transposer cette logique de régulation d'une activité illicite à celle de la sanction d'un acte illicite : la contrefaçon d'œuvres.

En effet, la fourniture d'un moyen d'expression en ligne ne peut réaliser l'infraction de contrefaçon qui se définit par l'illicéité du contenu mis à disposition. La sanction d'une telle fourniture de moyen est inefficace dès lors que nécessairement ces moyens évoluent. Ainsi de la même manière que le référé DADVSI de la loi du 1er août 2006 visant les procédés de P2P était déjà dépassé lors de son adoption[276] et qu'il a été décidé trois ans plus tard, dans le cadre de la loi HADOPI du 12 juin 2009, de mettre en place un référé visant non plus les logiciels d'échanges utilisant le réseau mais les services du web mettant en ligne les contenus[277], cette procédure est aujourd'hui questionnée alors que ces services sont volatiles et que le site de streaming bloqué aujourd'hui par une mesure de référé réapparaîtra demain.

Il a été vu dans cette étude que cette procédure de référé qui bloque un site à l'initiative de particuliers est inefficace et contraire au respect de la liberté de naviguer des internautes. Le blocage d'un site doit faire l'objet d'une mesure administrative. Certains s'interrogent alors sur un encadrement spécifique d'une telle activité dite de « streaming ».

Mireille Imbert-Quaretta, conseillère d'État, suggère ainsi la possibilité qu'une autorité administrative puisse adresser, à la suite d'une procédure contradictoire, une injonction de retrait prolongé au site hébergeant des contenus contrefaisant. Il est énoncé dans le rapport qui a été remis en 2014 que le champ d'application de cette mesure « *serait plus circonscrit que celui de l'article L336-2 du Code de la propriété intellectuelle, il ne concernerait que la persistance d'un contenu notifié ou la réapparition d'un tel contenu sur un site et ne pourrait viser que le retrait de ce contenu*

[276] Alors que cette formulation d'un logiciel *« principalement utilisé »* pour la mise à disposition illicite d'œuvres ou d'objets protégés par un droit d'auteur aurait du alerter sur son inefficacité, v. L336-1 du CPI.

[277] V. : L336-2 du CPI. Cet article a été crée par la loi du 12 juin 2009 et a été intégré dans un nouveau chapitre consacré à la *« Prévention du téléchargement et à la mise à disposition d'œuvres et d'objets protégés par le droit d'auteur et droit voisins* ». Sur l'efficacité du dispositif HADOPI qui organise par ailleurs la surveillance et la sanction des échanges sur les réseaux P2P, voir la position de Bruno ORY-LAVOLLEE, ancien directeur de la Société pour l'administration des droits des artistes musiciens et interprêtes (Adami), qui fait remarquer que : « *Il faut dès lors être conscient du fait que cette loi ne pourra combattre que les réseaux de pair à pair publics. Si elle le fait avec succès, le téléchargement illégal baissera au moins pour un temps. Mais il migrera des grands bazars gratuits du peer to peer vers des foires au troc locales, prenant souvent la forme de communications privées. »,* ORY-LAVOLLEE, « Création et Internet, inutile précaution ? », *Le Monde,* mardi 14 avril 2009.

déterminé »[278]. Une position qui apparaît déjà plus adéquate avec la nécessité d'un régime d'ordre public mais dont la faisabilité technique s'agissant du blocage d'un contenu déterminé seulement et non d'un site en son entier apparaît incertaine.

Or alors que l'on peut souligner que la mise à disposition de contenus s'oriente déjà vers de nouveaux procédés au carrefour du P2P et du streaming[279], il est difficile de la mettre en œuvre une procédure spécifique contre un procédé technique qui réalise un acte de contrefaçon ; la lutte contre celui-ci doit ressortir de la mise en œuvre de la responsabilité pénale de son auteur.

125. **Une politique de lutte contre les réseaux criminels de mise à disposition d'œuvres illicites**. La répression de sites réalisant une mise à disposition massive d'œuvres illicites doit faire l'objet d'une politique pénale visant d'abord le réseau criminel qui organise une telle activité de contrefaçon. En effet, il ne s'agit pas dans un premier temps de viser l'internaute contrefacteur qui télécharge un lien ; il est par ailleurs difficile d'envisager un régime administratif de blocage de tels sites à l'instigation de l'État français, qui devrait en supporter les coûts.

Ainsi d'une part, une politique de lutte doit viser le réseau criminel qui met à disposition un tel service. La difficulté est que celui-ci opère à l'échelle internationale en chiffrant ses données selon des schémas organisationnels qui favorisent d'autres infractions comme par exemple le blanchiment d'argent. Toutefois, l'exemple peut être pris de la fermeture par les États-Unis en janvier 2012 du site *Megaupload* et de l'arrestation en Nouvelle-Zélande de ses quatre fondateurs[280]. D'autre part, la logique de la notification et du retrait est efficace à cet endroit grâce notamment aux techniques de marquage d'œuvres. Des procédures spécifiques peuvent être mises en œuvre en application de lois visant la lutte contre la contrefaçon ; ainsi des « *DMCA Notice et Take down tools* » américains comme le « *Trust Copyright Removal Program* » de *Google* (autrement appelé « Fast track ») et l'emploi par Microsoft de « *DMCA*

[278] IMBERT-QUARETTA M., *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne, Rapport à Madame la ministre de la culture et de la communication*, mai 2014, p.16.

[279] Que sont les logiciels libres mettant en œuvre des moteurs de recherche spécialisés dans le référencement d'œuvres disponible en streaming sur le Web, tel « Cacaoweb ».

[280] V. le communiqué du département de la justice américain qui indique comment le ministère public a mis en cause sept individus et deux entreprises et attrait ceux-ci devant un grand jury pour infractions aux lois sur le copyright, «Justice Departement charges leaders of Megaupaload with widespread online copyright infringement », january 19, 2012, disponible sur le site www.justice.gov.

De la même manière, dans l'affaire qui oppose un FAI allemand et un producteur de film qui souhaite voir bloquer un site proposant ses œuvres en streaming, il est fait état de l'action de la police allemande à l'encontre de ses exploitants qui a permis que l'activité litigieuse cesse. Le juge européen relève cependant que « *la circonstance selon laquelle le site Internet en cause au principal a cessé son activité ne rend pas les questions préjudicielles irrecevables* » V. CJUE 27 mars 2014, aff. C-314/12 *UPC Telekabel Wien c/ Constantin Film Verleih Gmbh*.

Agents ». A cet endroit la HADOPI française est passée à côté de mesures efficaces dès lors qu'elle a opéré par mesures générales de retrait[281] laissant l'initiative de l'action aux individus et le choix de la mesure au juge.

Enfin, alors que la possibilité pour tous de s'exprimer à un public et donc de mettre à disposition de tous des œuvres apparaît comme la révolution induite par la création du réseau, il apparaît à cet endroit que les schémas de diffusion des œuvres et de rémunération des auteurs soient révolutionnés. Ainsi gageons que de la même manière qu'il apparaît aujourd'hui totalement désuet de télécharger des fichiers MP3 via un logiciel de P2P alors que le format du streaming couplé à la technique du pair-à-pair a permis l'émergence de services du type « *Spotify* » ou « *Deezer* » qui proposent une écoute illimitée de musique[282], le téléchargement ou le visionnage en streaming d'épisodes de séries ou de films fera place à l'abonnement à des services permettant un tel accès en illimité, qui peut être financé par le coût d'un abonnement comme par exemple aujourd'hui le service « *Netflix* » ou par le visionnage de publicité comme le propose par exemple « *YouTube* ». Les problématiques sont déjà celles de l'internationalisation des offres[283] qui doivent être accessibles à tous[284] sans que toutefois cela conduise à une uniformisation culturelle.

B] La mesure préventive visant la défense de l'ordre public

126. ***Plan***. La mesure de blocage d'un site peut avoir pour finalité la sauvegarde de l'ordre public, une mesure qui ressort donc d'un domaine où la police générale peut agir. Toutefois, il faut considérer que l'ordre public défendu ne peut être que spécial **(1)** et appréhender en ce sens la délimitation des mesures de blocage décidées à l'heure actuelle par la législateur français **(2).**

1) La spécialité de l'ordre public défendu

127. **Le non-sens d'un « ordre public numérique »**. Il faut souligner qu'on ne saurait spécifier l'ordre public à défendre sur le réseau par le seul qualificatif de numérique[285]. Celui-ci est en effet trop général : les enjeux ne peuvent tenir de la seule numérisation des échanges et des activités. Il faut affirmer qu'il s'agit bien de considérer les atteintes à la sûreté

[281] Article L336-2 du CPI.

[282] Et ce non pas du fait de la répression alors que déjà lors des débats de la loi DADVSI en 2006, la licence globale avait ses défendeurs et que le paiement d'une écoute ou son décompte dans le cas d'un forfait pour payer l'artiste était déjà envisagé.

[283] V. *infra* : « L'encadrement du blocage géographique »

[284] V. *supra* : « La mise en œuvre d'un accès pour tous ».

[285] Pour cette formule et la diversité des thèmes abordés, v. : *L'ordre public numérique, libertés, propriétés, identités,* Aix-en-Provence, PUAM : 2015, Ouvrage collectif Philippe Mouron et Carine Piccio (dir), (inter-normes coll.)

des individus dans le monde réel. La composante matérielle de l'ordre public qui renvoie au triptyque sécurité-tranquillité-salubrité n'est pas annihilée par l'immatérialité du réseau.

Disant cela, la problématique du contrôle à opérer émerge : il faut considérer les limites à la sanction de blocage d'un site et donc à la police qui la met en œuvre. Celle-ci ressort-elle de la nécessité d'établir un « *minimum de conditions qui apparaissent indispensables* » [286] pour garantir l'exercice de nos libertés et droits fondamentaux ? Doit-elle faire l'objet d'un pouvoir de police général ? La réponse est non.

La nouveauté du réseau et des échanges qu'il met en œuvre amène à considérer que les actions dont la puissance publique doit être investies sur celui-ci, ne peuvent ressortir que de pouvoirs de polices spéciaux fondés sur une habilitation législative. En effet l'habilitation opère la distanciation nécessaire à avoir alors que la réalité de l'atteinte ne peut être que ressentie et non directement constatée et qu'il faut noter par ailleurs qu'à l'endroit du réseau aucune circonstance particulière de temps et de lieu ne peut donner au pouvoir de police générale un caractère d'ordre « *contingent et relatif* »[287] contrôlé par le juge administratif. Le blocage d'un site, mesure automatique et absolue en ce sens qu'elle prive l'ensemble des individus de la consultation de celui-ci, ne peut se réaliser dans la mesure de sanction d'un pouvoir de police général au risque d'annihiler la liberté de naviguer sur le réseau[288]. De fait, actuellement deux types de sites peuvent faire l'objet d'une mesure de blocage administrative à titre préventif.

2) L'état de la législation actuelle visant la lutte contre la pédopornographie et le terrorisme

128. **L'habilitation législative de l'article 6-1 de la LCEN**. En 2011 la loi d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI 2 »[289], dans son chapitre intitulé « *Lutte contre la cybercriminalité* », introduit un nouvel alinéa à l'article 6-I-7 de la LCEN : l'autorité administrative peut requérir des FAI qu'ils bloquent l'accès à des services de communication au public en ligne dans le but de lutter contre la diffusion des images ou représentations de mineurs relevant de l'article 227-23 du Code pénal. La

[286] FRIER P.L., PETIT J., *Précis de droit administratif*, 5ème éd., Paris : Montchretien, Lextenso éditions, 2008 (Domat, droit public), n°410.

[287] *Ibid.*

[288] Il est à noter qu'il a été décidé que l'état d'urgence déclaré au lendemain des attentats, le 14 novembre 2016, a autorisé le Ministre de l'intérieur à « *prendre toute mesure pour assurer l'interruption de tout service de communication au public en ligne provoquant à la commission d'actes de terrorisme ou en faisant l'apologie* », v. l'article 11, II, de la loi n°55-385 du 3 avril 1955 relative à l'état d'urgence, telle que modifiée par la loi n°2015-1501 du 20 novembre 2015, article 4. Le rapport d'activité 2015 de la personnalité qualifiée prévue par l'article 6-1 de la loi n°2004-575 crée par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, détaillant le contrôle des mesures de blocage de sites entre mars 2015 et février 2016 mentionne que le ministre n'y a pas eu recours. Rapport disponible sur le site de la CNIL, cnil.fr.

[289] Loi 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

disposition a fait l'objet d'un recours devant le Conseil constitutionnel qui ne l'a pas censurée. Il était énoncé qu'un décret en Conseil d'État devait venir préciser les modalités d'application de ces mesures de blocage, notamment concernant la manière dont les surcoûts d'un tel blocage pour l'opérateur devaient être compensés. Ce décret n'a jamais été adopté.

La loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions de la lutte contre le terrorisme vise *« à renforcer les moyens de lutte contre la propagande terroriste, tant sur le plan de la procédure pénale qu'en matière de police administrative* »[290]. L'adoption du texte a fait l'objet d'une procédure accélérée engagée par le gouvernement ; la loi n'a pas fait l'objet de recours devant le Conseil constitutionnel. Dans le cadre du chapitre V s'intitulant « *Renforcement des moyens de prévention et d'investigations* » un nouvel article 6-1 est inséré dans la LCEN. Il permet à l'autorité administrative de demander aux FAI de bloquer l'accès aux sites non plus seulement dans le cadre de la lutte contre la pédopornographie mais s'agissant également de sites provoquant aux actes de terrorisme ou en faisant l'apologie, nouvelle incrimination introduite dans le Code pénal à l'article 421-2-5. Le décret d'application a été pris le 5 février 2015 ; il établit que les surcoûts liés au blocage des sites par les FAI feront l'objet d'une compensation financière par l'État[291]. Ce décret a fait l'objet d'un recours pour excès de pouvoir devant le Conseil d'État[292].

129. **La sortie critiquable de l'infraction de provocation et d'apologie au terrorisme du droit pénal spécial de la presse.** La nouvelle incrimination de la provocation et de l'apologie d'actes de terrorisme introduite dans le Code pénal à l'article 421-2-5[293] opère en la renforçant le transfert d'une disposition répressive déjà existante dans le droit français, prévue à l'alinéa 6 de l'article 24 de la loi sur la liberté de la presse du 29 juillet 1881[294].

---

[290] V. le dossier législatif disponible sur les sites assemblee-nationale.fr et Sénat.fr. V. également MBONGO Pascal *in L'ordre public numérique, libertés, propriétés, identités,* Aix-en-Provence, PUAM : 2015, Ouvrage collectif Philippe Mouron et Carine Piccio (dir), (inter-normes coll.), préface, p.16, qui souligne : « *Un texte qui ne s'intéressait pour sa part principalement qu'à la maîtrise par l'État des circulations de certains individus suspects de la radicalisation islamiste* ».

[291] Décret 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

[292] Conseil d'État, n°389140, 2ème/7ème SSR, lecture du lundi 15 février 2016.

[293] Code pénal : « *Art. 421-2-5 - 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 75000€ d'amende.*

« Les peines sont portées à sept ans d'emprisonnement et à 100000€ d'amende lorsque les faits 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, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.»

[294] « *Seront punis des peines prévues à l'alinéa 1er ceux qui par les mêmes moyens énoncés en l'article 23, auront provoqué directement aux actes de terrorisme prévus par le titre II du livre IV du code pénal, ou qui en auront fait l'apologie* », ancien alinéa 6 de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse, désormais supprimé par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à lutte contre le terrorisme, qui crée dans le code pénal l'article 421-2-5.

Le choix qui a été fait de sortir cette incrimination de la loi sur la liberté de la presse du 29 juillet 1881 peut être critiqué en ce sens que même si l'on comprend qu'il ne s'agit plus de viser en premier lieu la communication d'un acte pénalement réprimé mais bien de pénaliser le comportement de provocation à des actes de terrorisme ou d'apologie de ces actes, l'exégèse apparaît spécieuse. Elle révèle que ce procédé vise en réalité à enserrer les mesures de blocage par la création d'une infraction pénale, croyant justifier celles-ci par la création de celle là. Or au contraire ces mesures de blocage gagneraient à répondre d'une police administrative spéciale qui détaillerait ses objectifs et donc les contours de l'ordre spécial défendu ; alors que par ailleurs il est dommageable que ne subsiste pas une infraction de communication de telles idées. Un site engageant à faire le Djihad doit être bloqué, faire l'apologie dans l'espace public ou sur un blog des actes terroristes perpétrés doit être sanctionné sur le terrain de la liberté d'expression et de ses limites[295] et selon la procédure pénale protectrice des délits de presse[296].

130. **La défense d'un ordre public spécial**. Dans l'étude d'impact jointe au projet de loi, il est établi un « *constat alarmant* »[297] : « *Internet constitue aujourd'hui le vecteur principal de la propagande, du recrutement et de l'incitation au terrorisme* »[298]. Emergent ici les objectifs d'une police administrative spéciale visant non pas la provocation ou l'apologie du terrorisme mais les sites de « *propagande* », de « *recrutement* », et « *d'incitation au terrorisme* ». La détection de ceux-ci et leur blocage doivent répondre d'un choix politique en vue de la défense de l'ordre public non pas numérique mais matériel. En ce sens, la mesure ne peut être fondée sur la définition d'une infraction pénale dès lors que son but est préventif.

L'on peut souligner également que si certains peuvent s'étonner de voir accoler deux objectifs différents tels la lutte contre la pédopornographie et la lutte contre le terrorisme, les troubles qui sont visés répondent de la même logique. L'État fait acte de

[295] En ce sens il faut critiquer pour leur caractère disproportionné les condamnations qui se sont multipliées en France après les attentats de janvier 2015 à l'encontre d'auteurs de propos ou de messages faisant l'apologie du terrorisme, condamnés à de la prison ferme pour certains d'entre eux. V. MANENTI Boris, « Apologie du terrorisme : une longue liste de condamnations », article mis en ligne le 20 janvier 2015 sur le site nouvelobs.com, et SOULLIER Lucie, « Dans le grand fourre-tout de l'apologie du terrorisme », article mise en ligne le 21 décembre 2015, sur le site lemonde.fr.

Comme le souligne le professeur Emmanuel Derieux s'agissant de ces condamnations « *Mal comprises, elles ne pourraient que radicaliser les terroristes, leur fournir des arguments ou faire leur jeu* », DERIEUX E., « Provocations et apologie du terrorisme », *Revue européenne des médias et du numérique*, n°33, hiver 2014-2015, p.5.

[296] Le transfert dans le Code pénal a une incidence sur la procédure alors que l'infraction n'étant plus soumise aux règles procédurales spéciales du droit de la presse, les poursuites n'obéissent plus notamment aux délais spécifiques de prescription de l'action, aux formalités à respecter et aux délais de jugement. La comparution immédiate est ainsi possible.

[297] LAZERGUES Christine, « La lutte contre le terrorisme peut-elle mettre en danger la liberté d'expression ? », *Légipresse*, n°321, novembre 2014, p.579.

[298] Etude d'impact, NOR : INTX1414166L/Bleue,-18 juillet 2014, v. le dossier législatif du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme disponible sur le site de l'Assemblée nationale, assemblee-nationale.fr

souveraineté devant la montée de réseaux criminels internationaux. Une mise en œuvre de sa puissance légitime tant qu'elle obéit aux limites de la défense de cet ordre public spécial, ce qui est contrôlé par le juge constitutionnel.

§2) Le contrôle de la mise en œuvre d'une telle mesure de police administrative spéciale

131. ***Plan.*** Il est souvent affirmé qu'une mesure de blocage ne peut être mise en œuvre que par le juge judiciaire. Ce qui est inexact **(A).** La défense de nos libertés eu égard aux mesures prises par l'administration relève des juges constitutionnel et administratif **(B).**

A] L'incompétence du juge judiciaire

132. **L'incompétence du juge judiciaire**. D'une part, par un raccourci dangereux si ce n'est grossier[299], affirmer que le blocage d'un site ressort de la compétence exclusive du juge judiciaire conduit à considérer que la seule décision du juge judiciaire vient légitimer toute mesure de blocage comme dans le cas, par exemple, d'instances à l'initiative d'ayant-droits qui en référé demandent une telle mesure pour faire cesser le trouble[300]. Or il a été démontré qu'une telle action méconnait le principe de la liberté de naviguer sur le réseau alors que toute restriction à celle-ci ne peut ressortir que des pouvoirs publics. De fait l'analyse de la proportionnalité de l'atteinte et de l'équilibre entre les droits fondamentaux en cause à l'échelle de mesures ordonnées en référé doit alerter sur l'incompétence du juge judiciaire à cet endroit dès lors qu'il apparaît que le contrôle de conventionalité est systématique [301].

---

[299] Le raccourci tend à être fait puisque les juges eux-mêmes requièrent cette mesure dans le cas de procédures de référés, alors qu'ils se déclarent dans le cadre d'une instance sur requête ou en référé incompétents pour couper l'accès au réseau. V. pour une décision en ce sens, TGI Paris, ord. réf. 8 octobre 2004, Juris-Data n°2004-254145, « *Attendu enfin que la mesure sollicitée à savoir la résiliation d'une convention permettant l'accès à internet ne ressort pas de la compétence du juge des requêtes, ni d'ailleurs de celle du juge des référés* ».

[300] V. ainsi : Olivier Pignatari qui énonce « *S'il on peut se féliciter du rôle central reconnu au juge –garant des libertés individuelles-dans le dispositif de protection de la création, il ne faut pas négliger le fait, qu'une fois de plus, la technique risque d'aller plus vite que la réponse judiciaire* », dans une instance qui traitait de la demande de groupements de professionnels du cinéma et de la vidéo aux fins de bloquer des sites de streaming, O. PIGNATARI « Blocage et déréférencement de plusieurs sites de streaming : à qui profite le stream ? », note sous TGI Paris, réf. 28 nov. 2013, *RLDI* 2013/99, n°3293.

De la même manière, il est difficile d'approuver Christophe Caron qui énonce « *En effet, seul le juge judiciaire est en mesure de concilier les droits et libertés fondamentaux que sont le droit d'auteur, la liberté d'expression et la liberté d'entreprendre. Et il est dangereux de laisser à une partie, que ce soit le demandeur ou l'intermédiaire, le soin d'apprécier unilatéralement cette conciliation ô combien délicate* », car il apparaît que pour éviter cette conciliation unilatérale en dehors de toute procédure judiciaire la mention du recours au juge ne suffit pas dès lors que les FAI peuvent être tentés pour éviter le coût d'une action en justice de faire droit aux demandes des ayants-droit. Les mesures de blocage doivent être d'ordre public pour éviter cela. V. CARON C., « Le blocage des sites contrefaisants une nouvelle fois devant la Cour de justice de l'Union européenne », *CCE,* 2014, comm. 43.

[301] Voir pour cette approche circonstanciée : TGI Paris, réf. 28 nov. 2013, disponible sur le site legalis.net. *Contra* pour un refus de toute appréciation mais selon une formulation dès lors éclairante : « *Attendu qu'il ne nous appartient pas de porter appréciation, comme le suggèrent les sociétés AOL France, France Télécom ou Tiscali Accès, sur la conformité du dispositif à envisager aux principes constitutionnels […]* », v. TGI Paris, réf. 13 juin 2005, *UEJF et al c/ Free, AOL et al,*disponible sur le site legalis.net.

De la même manière, dans le cas des instances européennes, l'on peut s'étonner que dans le cas d'une demande de blocage d'une communication, que ce soit un flux P2P ou une requête vers un site, la CJUE indique qu'il faille opérer une conciliation non pas entre deux intérêts mais entre trois : la mesure de blocage doit assurer un juste équilibre entre « la

Toutefois la problématique n'est pas non plus celle de la nécessité de recourir au juge judiciaire dans le cas de la mise en œuvre de mesures d'ordre public. Le débat est actuellement ici celui « *du périmètre de la compétence du juge judiciaire en tant que gardien de la liberté individuelle* » ou « *des libertés individuelles* »[302]. Le juge judiciaire est fondé originellement en application de l'article 66 de la Constitution à contrôler l'action de l'administration en ce domaine, son indépendance en faisant l'arbitre nécessaire des enjeux en présence. Cependant les mesures de blocage mises en œuvre par des polices spéciales apparaissent ici comme des restrictions au principe de liberté de navigation. Il n'est pas porté atteinte à la liberté d'accès au réseau et ces mesures n'ont donc pas à être mises en œuvre par le juge judiciaire[303].

Il faut ainsi considérer que le choix du recours au président du TGI dans le cadre de la procédure de blocage initiée par le président de l'ARJEL est malvenu en ce qu'il empêche toute réflexion autour de l'étendue des pouvoirs de police de l'administration, qui doivent faire l'objet d'un contrôle[304].

---

protection du droit de propriété intellectuelle », le protection de « *la liberté d'entreprise du FAI* » et « *la protection des droits fondamentaux des clients du FAI* », notamment leur droit à la protection de leurs données personnelles et leur liberté de recevoir ou de communiquer des informations (V. CJUE 24 novembre 2011, aff. C-70/10 *Scarlet Extended Sa c/ SABAM*). La mention d'une protection des droits fondamentaux dans leur ensemble *« des clients »* du FAI doit être critiquée alors que ces considérations ne peuvent être mises à la charge de l'opérateur. L'impasse relevée est révélatrice du changement d'échelle à opérer. De fait dans une décision ultérieure, est considérée la *« liberté d'information des utilisateurs d'Internet* », et le juge européen qui enjoint à des mesures de blocage strictement ciblées précise que « *les juridictions nationales doivent avoir la possibilité de vérifier que tel est le cas* » alors pourtant qu'elles les ont requises mais que pour ménager la liberté d'entreprendre du FAI leur nature est laissée à l'appréciation de l'opérateur (V. et CJUE 27 mars 2014, aff. C-314/12 *UPC Telekabel Wien c/ Constantin Film Verleih Gmbh*).

[302] B. LOUVEL, 1er président de la Cour de cassation, « L'autorité judiciaire, gardienne de la liberté individuelle ou des libertés individuelles ? Réflexion à l'occasion de la rencontre annuelle des premiers présidents de cour d'appel et de la Cour de cassation », le 3 février 2016, disponible sur le site de la Cour de cassation, www. courdecassation.fr

[303] La définition que donne le conseiller d'État, Jean-Eric Schoettl, peut être rappelée ici : « *la police administrative : - se rattache non à la répression d'une infraction déterminée, mais à la protection de l'ordre public et à la prévention des infractions. Sa raison d'être est d'éviter ou de faire cesser un trouble, fût-il constitutif d'une infraction. –est susceptible d'affecter la liberté de la personne (droit d'aller et venir, enregistrement des données personnelles, etc.), mais n'implique ni rétention, ni détention. ».* Le conseiller d'État le rappelle : « *La vision dogmatique assimilant toute restriction de la liberté personnelle (du fait de la police administrative) à une atteinte à la liberté individuelle au sens de l'article 66 de la Constitution, et appelant dès lors l'intervention du juge judiciaire, se heurterait à de manifestes impossibilités pratiques. Ainsi pour prendre l'exemple de la liberté d'aller et venir, va-t-on soumettre à l'agrément préalable du juge judiciaire toute mise en sens unique d'une voie de circulation ? L'installation de tout panneau de limitation de vitesse ? Il faut donc se rendre à l'évidence et respecter la summa divisio existant dans toutes les démocraties entre prévention et répression, police administrative et judiciaire », v. :* J.E.- SCHOETTL, *Gaz.Pal.*, 7 février 2006, n°38, p.20, note sous Conseil constitutionnel n°2005-532 DC (Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers).

[304] Ainsi il nous semble qu'il ne s'agit pas de souligner comme le fait Anne Debet qu':«*il s'agit d'une mesure prononcée par un juge ce qui en soi est une garantie très forte »*, v. A. DEBET, « Refus de transmission de QPC par les jeux en ligne par la Cour de cassation », *CCE* 2013, comm.114. Elle rappelle alors que les débats parlementaires avaient vu le rapporteur devant l'Assemblée nationale soumettre une compétence exclusive de blocage à l'ARJEL, une *« hypothèse de filtrage administratif qui a fait long feu tant elle a suscité des désaccords au sein du Parlement »*, v. A. DEBET, *ibid.*

De la même manière souhaiter comme la Commission Nationale Consultative des Droits de l'Homme que les mesures de blocage de sites soient confiées au « juge de la liberté et de la détention » qui serait nommé le « juge des libertés » est une proposition rhétorique, v. LAZERGUES Christine, « La lutte contre le terrorisme peut-elle mettre en danger la liberté d'expression ? », *Légipresse*, n°321, novembre 2014, p.579.

B] Les contrôles du juge constitutionnel et du juge administratif

133. ***Plan***. Il faut souligner dans un premier temps que l'opportunité de la mesure est du ressort du législateur qui vote la loi d'habilitation. Puis le contrôle du bien-fondé de telles polices est du ressort du Conseil constitutionnel **(1)** et le contrôle de la mise en œuvre de leurs contenus relève du juge administratif **(2).**

1) Le contrôle de l'étendue de l'habilitation législative par le juge constitutionnel.

134. **La garantie du respect des libertés fondamentales de l'individu.** Il faut rappeler que l'action de blocage d'un site agit sur le réseau et non sur l'individu. Bloquer un site est une restriction à la liberté de naviguer des citoyens français mais n'obère pas à elle seule cette liberté. Il en va différemment de la décision de priver un individu de son accès ou de filtrer les sites auxquels il peut accéder ; ici alors qu'est en jeu la sûreté de l'individu et sa liberté même de déplacement, l'intervention du juge judiciaire est nécessaire.

Cette logique appert dans la décision du Conseil constitutionnel amené à se prononcer sur le régime administratif des mesures de blocage visant les sites pédopornographiques décidé par la LOPPSI en 2011[305] sans toutefois que l'articulation soit claire dès lors que l'appréciation de l'atteinte à la liberté de communication fait encore écran, comme dans la décision de 2009 sur la loi HADOPI[306], entre la mesure visant ici l'accès à un site et la sauvegarde de l'ordre public.

Ainsi les juges de la rue Montpensier énoncent que « *les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne* ». Toutefois ils fondent leur contrôle ainsi : « *ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclarations des droits de l'homme et du citoyen de 1789* »[307]. Or comme le souligne

[305] V. la décision du Conseil constitutionnel du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure,* n°2011-625 DC. Il est à noter qu'elle est la seule décision des juges de la rue Montpensier qui traite de mesures de blocage de sites, dès lors que le Conseil constitutionnel n'a pas été saisi de la loi du 2014-1353 du 13 novembre 2014 renforçant les dispositions de lutte contre le terrorisme, et que sa saisine s'agissant de la loi n° 2010-476 « *relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne* » n'a pas soulevé cette problématique dès lors que la mesure était confiée à l'autorité judiciaire (V. Décision n°2010-605 DC du 12 mai 2010).

[306] Décision n°2009-580 du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur internet.*

[307] Décision n°2011-625 du 10 mars 2011 DC, cons. 8. Le commentaire aux Cahiers indique ainsi que « comme le rapporteur au Sénat le rappelait , "la disposition proposée présente une portée beaucoup plus restreinte puisqu'elle tend non à interdire l'accès à internet mais à empêcher l'accès à un site déterminé en raison de son caractère illicite"[307] (Jean-Patrick Courtois, Rapport fait au nom de la Commission des lois sur le projet de loi, adopté par l'Assemblée nationale, d'orientation et de programmation pour la performance de la sécurité intérieure, Sénat, session ordinaire de 2009-2010, n°517, 2 juin 2010, p.47.) »

très justement David Ginocchi : « *Si l'on se place du côté de l'utilisateur d'internet, il apparaît en effet que l'atteinte à la liberté de communication est moins grave lorsque l'accès à un site est interdit que lorsque toute connexion au réseau est interdite. En revanche, si l'on se place du côté de celui qui est à l'origine du site bloqué, l'atteinte consiste bien dans la privation « de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile » qui rendait justement nécessaire l'intervention du juge judiciaire dans la décision de 2009 (cons. 16)* »[308].

Le raisonnement de la décision HADOPI de 2009 déjà critiquable ne peut plus tenir[309]. Le Conseil constitutionnel doit s'assurer de la sauvegarde de la liberté de naviguer sur le réseau, envisagée comme une nouvelle modalité de la liberté d'aller et venir.

135. **L'appréciation du point d'équilibre**. Le juge constitutionnel doit ainsi apprécier que la mesure de blocage ménage un équilibre entre la liberté de naviguer sur le réseau et la défense de l'ordre public spécial visé[310].

Ainsi d'une part, le juge constitutionnel doit apprécier la spécialité de la police administrative. En ce sens, pour l'instant, le contenu des polices sanctionnées par des mesures de blocage est délimité s'agissant d'une activité réglementée, l'activité des jeux d'argent et de hasard en ligne, et de deux types de troubles que constituent la mise en ligne de sites pédopornographiques et la mise en ligne de sites provocant à des actes de terrorisme ou en faisant l'apologie. Dans sa décision 2011-625 DC du 10 mars 2011 s'agissant de la LOPPSI, le Conseil constitutionnel énonce ainsi que les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre l'accès à des services de communication au public en ligne *« lorsque et dans la mesure où il diffuse des images de pornographie infantile »*[311].

D'autre part, le juge constitutionnel doit apprécier la réalité de l'atteinte à l'ordre public envisagée. Cette appréciation permet de limiter la multiplication de telles polices administratives spéciales dont la sanction est le blocage de sites. Ainsi si l'on

[308] GINOCCHI D., « Le contrôle de la LOPPSI par le Conseil constitutionnel », AJDA 2011, p. 1097

[309] V. *supra* le chapitre 2 intitulé : « *La reconnaissance du caractère fondamental de ce nouveau principe* », Section I *« Le possible rattachement à la liberté individuelle »*.

[310] V. David Ginocchi qui rappelle la décision du Conseil constitutionnel du 25 janvier 1985, *Loi relative à l'état d'urgence en Nouvelle-Calédonie*, n°85-187 DC (JO 26 janvier 1985, cons. 3 ; *GDCC*, 15ème éd. 2009, n°29), qui énonce que le Conseil constitutionnel est chargé de s'assurer que les dispositifs de police institués par la loi permettent « *d'opérer la conciliation nécessaire entre le respect des libertés et la sauvegarde de l'ordre public sans lequel l'exercice des libertés ne saurait être assuré* », GINOCCHI D., « Le contrôle de la LOPPSI par le Conseil constitutionnel », *AJDA* 2011, p. 1097. Sur l'extension progressive du contrôle de constitutionnalité s'agissant des lois de police spéciale, v. également : FRIER P.L., PETIT J., *Précis de droit administratif*, 5ème éd., Paris : Montchretien, Lextenso éditions, 2008 (Domat, droit public), n°431.

[311] V. la décision du Conseil constitutionnel du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, n°2011-625 DC (cons.8).

pressent l'atteinte à la sécurité dans le cadre de polices spéciales adoptées à ce jour visant la pédopornographie et la propagande terroriste, il en va par exemple différemment d'une proposition qui en 2013 souhaitait voir envisagé le blocage de sites de proxénétisme[312]. Alors qu'il ne peut s'agir de règlementer ce type d'activités, il est difficile de considérer que l'atteinte relève de la sauvegarde de l'ordre public, c'est-à-dire qu'elle relève de la nécessité d'un acte préventif[313].

136. **La nécessité d'une procédure de contrôle de la mesure mise en œuvre.** Dans sa décision 2011-625 DC du 10 mars 2011 s'agissant de la LOPPSI, sur la possibilité de mettre en œuvre un blocage administratif des sites pédopornographiques, le Conseil constitutionnel prend en compte dans son appréciation de l'équilibre à mettre en œuvre le fait que « *la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé* »[314].

En effet il faut rappeler utilement comme le fait le professeur Wachsmann que *« les garanties offertes, par les deux ordres de juridiction sont en effet équivalentes au regard des normes définissant l'équité du procès* »[315]. Or cette équité est recherchée mais suivant des procédures inefficaces. Ainsi dans l'arrêt de la CJUE dit « Telekabel » du 27 mars 2014, le juge européen affirme qu'«*il est nécessaire que les règles nationales de procédure prévoient la possibilité pour les internautes de faire valoir leurs droits devant le juge une fois connues les mesures d'exécution prise par le fournisseur d'accès* » [316]. Le professeur Caron commentant cette précision « *originale et nouvelle* » mentionne alors la procédure de la tierce-opposition des articles 582 et suivants du CPC[317]. Toutefois, même s'il s'agit d'une « *fausse voie de recours extraordinaire* »[318] alors que le tiers peut l'initier contre tout jugement[319], y compris contre une ordonnance de référé, il faut que le tiers y ait un intérêt. Or sur le plan civil il faut constater que les demandes d'intervention volontaire de particuliers dans les

[312] V. « Le Gouvernement renonce à filtrer les sites de prostitution» sur l'amendement déposé à la proposition de loi contre la prostitution défendu par Fleur Pellerin, *RLDI,* actualités, n°99, déc. 2013, p.47.

[313] Ainsi dans le même sens, dans le commentaire aux Cahiers, s'agissant de la décision n°2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI),* il est souligné pour différencier le blocage décidé ici des mesures prises dans le cadre de la HADOPI : «*il s'agit également de lutter contre l'exploitation sexuelle des mineurs, ce qui peut justifier des mesures que la préservation de propriété intellectuelle ne peut fonder ».*

[314] V. la décision du Conseil constitutionnel du 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure,* n°2011-625 DC (cons.8).

[315] WACHSMANN Patrick, « De la marginalisation du juge judiciaire en matière de libertés et des moyens d'y remédier », *D.* 3mars 2016, n°9, éditorial.

[316] CJUE 27 mars 2014, *aff.* C-314/12 *UPC Telekabel Wien c/ Constantin Film Verleih Gmbh*, cons. 57.

[317] CARON C., « Le blocage des sites contrefaisants une nouvelle fois devant la Cour de justice de l'Union européenne », *CCE,* 2014, *comm.* 43

[318] CADIET L., JEULAND E., *Droit judiciaire privé,* 7ème éd., Paris : LexisNexis, 2011 (Manuel), n° 862.

[319] Article 582 du CPC.

instances qui opposaient des ayant-droits ou des associations de défense de droits et les FAI n'ont pas été reçues par le juge judiciaire qui ne pouvait de fait caractériser à ce niveau un intérêt légitime. Ainsi à l'audience de référé du 30 mai 2005 présidée par Emmanuel Binoche, dans l'affaire dite « *aargh* », il est ainsi énoncé pour rejeter une telle intervention, très pertinemment, mais sans que le paradoxe soit relevé : « *qu'en réalité ceux-ci prétendent par cette démarche se substituer à cette juridiction dans l'appréciation des demandes qui lui sont soumises* ». La formulation éclaire pourtant sur la nécessité d'un contrôle de légalité à l'initiative du citoyen alors que la mesure de blocage le vise et ne relève pas d'un conflit privé entre deux entités.

Ainsi il faut s'interroger également sur la création, par la loi du 13 novembre 2014 renforçant les dispositions de lutte contre le terrorisme, d'un référé pénal spécial à l'article 706-23 du Code de procédure pénale, visant les infractions de l'article 421-2-5 et permettant au juge pénal d'arrêter tout service de communication en ligne lorsqu'il constitue un trouble manifestement illicite, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir[320]. Le recours au juge judiciaire quand bien même pénal n'assure pas davantage le respect des libertés fondamentales des citoyens dans le cadre de la mise en œuvre de mesures qui ont vocation à s'appliquer à l'ensemble de la population française, ce qui semble dénier toute utilité à la mention faite ici de l'intérêt à agir[321]. Utilement toutefois ce référé renvoie à la nécessité que des sites réalisant l'infraction de provocation et d'apologie du terrorisme puissent être facilement portés à la connaissance des pouvoirs publics. On rappellera à cet endroit que des plateformes de signalement mises en œuvre par les pouvoirs existent[322].

Il convient donc de restaurer le contrôle du juge administratif, dont les conditions de saisie et de contrôle sont efficaces eu égard à la nature de l'atteinte opérée.

2) Le contrôle de la légalité de la mesure prise par le juge administratif

137. **Le recours pour excès de pouvoir dirigé contre les décrets d'application de l'article 6-1 de la LCEN.** Il faut apprécier que cette action restaure un contradictoire utile alors que l'intérêt à agir pour le recours pour excès de pouvoir est plus largement entendu dès

[320] V. le nouvel article 706-23 du Code de procédure pénale, créé par la loi 2014-1353 du 13 novembre 2014 renforçant les dispositions de lutte contre le terrorisme.

[321] Il est à noter que dans les commentaires aux Cahiers, s'agissant de la décision n°2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI)*, il est souligné pour différencier le blocage décidé ici des mesures prises dans le cadre de la HADOPI qu' « *il s'agit de protéger les utilisateurs internet d'eux-mêmes* ».

[322] V. : La plateforme dite « Pharos » : www.internet-signalement.gouv.fr,

lors que l'appréciation se fait « *au regard du droit objectif pour assurer le respect du principe de légalité* » [323]. Ainsi dans sa décision du 15 février 2016 se prononçant sur le recours pour excès de pouvoir introduit par plusieurs associations contre le décret n°2015-125 du 5 février 2015 venant préciser la procédure de blocage de sites provoquant à des actes de terrorisme ou pédopornographiques, le Conseil d'État déclare recevable l'intervention de la société « *Article 19* », une société qui n'est pas un fournisseur d'accès mais une association qui défend la liberté d'expression et d'information, en soulignant qu'elle justifie « *d'un intérêt suffisant* »[324].

L'action des requérants tend alors à ce que soit opéré le contrôle de conventionalité des nouvelles possibilités de blocage de sites introduites par la loi du 13 novembre 2014. Sur le fondement de l'article 10 de la CEDH, le Conseil d'État conclut que les restrictions opérées à la liberté d'expression sont prévues par la loi, poursuivent des objectifs légitimes et ne sont pas disproportionnées[325]. Par ailleurs plus utilement, il rappelle, alors que les requérants arguaient également de la méconnaissance de l'article 6 de la Conv. EDH « Droit à un procès équitable », que les dispositifs de blocage « *constituent des mesures de police administrative ; que par suite, et en tout état de cause, ni le principe des droits de la défense, ni les stipulations du paragraphe 1 de l'article 6 de la Convention européenne des sauvegarde des droits de l'homme et des libertés fondamentales ne peuvent être utilement invoqués* »[326].

De fait une procédure de contrôle non juridictionnelle du contenu des mesures prises est instituée.

138. **Le contrôle non juridictionnel du contenu des mesures prises par l'administration dans le cadre de cette police spéciale**. Il apparaît que la liste des sites bloqués à la demande de l'autorité administrative pour des raisons évidentes de confidentialité[327] ne peut faire l'objet de publicité. Dès lors il faut s'interroger sur les conditions du contrôle non juridictionnel institué.

---

[323] FRIER Pierre-Laurent, PETIT Jacques, *Droit administratif*, 9ème éd., LGDJ Lextenso Editions : 2014, (Domat droit public), n°847.

[324] CE n°389140, 2ème /7ème SSR, lecture du lundi 15 février 2016.

[325] *Ibid.*, cons. 11 à 16.

[326] *Ibid*, cons. 19.

[327] V. pour « *le mode de transmission sécurisé, qui en garantit la confidentialité et l'intégrité* » et l'obligation pour les FAI de préserver « *la confidentialité des données qui leur sont ainsi confiées* », le décret n°2015-125 du 5 février 2015. Par ailleurs le rapport de la personnalité qualifiée pour l'année 2015 souligne qu'« *il a été constaté qu'à la suite du blocage de sites pédopornographiques, de nouveaux sites identiques apparaissaient, avec une adresse légèrement modifiées* », ce qui invite bien à prescrire que les adresses initiales ne doivent pas faire l'objet de publicité (Rapport d'activité 2015 de la personnalité qualifiée prévue par l'article 6-1 de la loi n°2004-575 créé par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, Alexandre Linden, du 15 avril 2016, disponible sur le site de la CNIL, p. 13).

Le nouvel article 6-1 de la LCEN créé par la loi du 13 novembre 2014 renforçant les dispositions de lutte contre le terrorisme prévoit que les demandes de retrait de sites de l'OCLCTIC[328] sont transmises à une personnalité qualifiée, dont il a été décidé qu'elle serait désignée au sein de la CNIL. Celle-ci s'assure de leur régularité et le cas échéant recommande à l'autorité administrative d'y mettre fin. Si cette recommandation n'est pas suivie, la personnalité qualifiée est compétente pour saisir la juridiction administrative en référé ou sur requête[329].

Or il peut être souligné que le choix de la CNIL pour s'assurer de la régularité des demandes de blocage ne va pas de soi alors qu'il n'est pas question ici de considérer le traitement de données à caractère personnel. Ce choix atteste de l'évolution de ses pouvoirs qui positionne l'autorité administrative indépendante comme l'acteur des problématiques de « *l'informatique* » et des « *libertés* », ce qui est bien vaste. Peut-être pour plus de clarté, aurait-il fallu considérer la création d'une instance de contrôle spécifique, qui aurait été davantage visible ne serait-ce que par le nom qu'on aurait pu lui donner. En effet, qui sait qu'Alexandre Linden[330] est la *« personnalité qualifiée prévue par l'article 6-1 de la loi n°2004-575 créé par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme* » et quelle visibilité a le premier rapport d'activité qu'il a rendu le 15 avril 2016 [331]?

139. **Les rapports d'activité de la personnalité qualifiée.** De fait, ce premier rapport publié en 2016 préconise de désigner un suppléant à la personnalité qualifiée, de renforcer les moyens mis à sa disposition alors que pour l'instant le dispositif s'appuie sur des personnels de la CNIL qui « *outre leur activités habituelles, se relaient par équipe de deux, pour apporter leur concours à la personnalité qualifiée* », d'améliorer les modalités techniques de mise à disposition des listes, préconisation qui témoigne de la technicité des mesures dont le contrôle devrait relever d'une appréciation collégiale et multidisciplinaire ; il y est enfin

[328] Le décret n°2015-125 du 5 février 2015 désigne l'Office Central de Lutte Contre la Criminalité liée aux Technologie de l'Information et de la Communication (OCLCTIC), rattaché à la direction nationale de la police nationale et donc au ministère de l'Intérieur.

[329] Article 6-1 alinéa 3, Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Le 1er rapport de la personnalité qualifiée pour l'année 2015 (mars 2015-février 2016) indique que les décisions de l'OCLCTIC ont donné lieu à deux recours gracieux rejetés. La recommandation de la personnalité qualifiée ayant été suivie, la juridiction administrative n'a eu à connaître d'aucun contentieux. Rapport d'activité 2015 de la personnalité qualifiée prévue par l'article 6-1 de la loi n°2004-575 crée par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, Alexandre Linden, du 15 avril 2016, disponible sur le site de la CNIL, p. 13

[330] M. Alexandre Linden est conseiller honoraire à la Cour de cassation.

[331] *Ibid.* Il est à noter que le rapport est disponible sur le site de la CNIL (cnil.fr) à partir de son moteur de recherche, mais l'on peut s'étonner que l'organigramme du site à la date du 30 juin 2016 ne fasse pas apparaître la mention de cette personnalité qualifiée et de ses fonctions. V. également sur ce rapport : « CNIL : Contrôle du blocage administratif des sites : 1er rapport de la personnalité qualifiée », *RLDI*, actualités, n°126, 2016.

souligné la nécessité de prévoir « *les modalités règlementaires de contrôle auprès des différents acteurs du dispositif institué par l'article 6-1 de la loi du 21 juin modifiée* ».

Il convient en effet de prendre conscience de la réalité du contrôle à opérer et de considérer qu'il ne s'agit pas simplement de vérifier une liste de noms de domaine et de sites bloqués. L'enjeu démocratique eu égard à la liberté de naviguer de tous doit amener à une visibilité accrue de cette nouvelle instance de contrôle et de ses missions, et à l'allocation de moyens en conséquence. Cette nécessité est rappelée dans le dernier rapport d'activité de 2017 publié le 30 mai 2018 qui souligne l'augmentation des demandes de blocage et de retraits de contenus à caractère terroriste. Il est souligné que la question des moyens mis à disposition de la personnalité qualifiée devient cruciale[332].

[332] V. : « Rapport d'activité 2017 de la personnalité qualifiée prévue par l'article 6-1 de la loi n° 2004-575 du 21 juin 2004, créé par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, mars 2017-février 2018, M. Alexandre Linden», rapport disponible sur le site de la CNIL, www.cnil.fr

Conclusion Chapitre 1er

140. **La libre-navigation de l'internaute**. Une fois l'accès au réseau garanti à l'internaute, il doit être affirmé, dans un second temps, un principe de libre-navigation sur son application web. Un État dit « *de droit* » ne peut en effet décider de limiter arbitrairement les points du réseau accessibles à ses citoyens. L'individu doit être libre de circuler sur le réseau et ne peut être restreint dans ses choix de connexions d'une manière telle que serait nié son droit d'accès au réseau.

Ce principe de liberté appelle à un régime le mettant en œuvre. Il ne s'oppose pas, bien au contraire, à une immixtion étatique. En effet la sauvegarde de cette liberté implique que le réseau soit gouverné : les activités qui s'y développent doivent faire l'objet d'une surveillance et les troubles à l'ordre public doivent être prévenus. Les acteurs privilégiés de cette surveillance sont les FAI qui doivent participer de la détection de certaines activités illicites et mettre en œuvre les politiques publiques de lutte contre les nouveaux aspects de la criminalité. Pour ce faire, les pouvoirs publics peuvent ordonner des mesures de blocage.

141. **La nature administrative de la mesure de blocage**. Il faut affirmer fermement que eu égard au respect de la liberté de navigation de tout internaute sur le réseau, la mesure de blocage d'un site ne peut ressortir d'une initiative privée quand bien même celle-ci est ordonnée par le juge judiciaire. En effet notamment dans le cadre du contexte de la lutte contre le téléchargement illégal visant des sites dits de « *streaming* », les actions d'ayant-droits se sont multipliées, pour requérir sur le fondement du référé spécial de l'article L336-2 du CPI le blocage d'un site proposant des liens renvoyant à des œuvres contrefaites.

Or cet usage du référé méconnait non seulement les fondements civilistes, en ce que la recherche de la responsabilité de l'auteur du trouble est absorbée par celle de l'efficacité de sa cessation, mais elle méconnait également la liberté fondamentale de naviguer sur le réseau pour l'individu alors que la mesure de police de blocage d'un site doit relever nécessairement d'une politique publique obéissant à un régime défini, transparent et contrôlé. L'action du juge judiciaire n'est pas en tant que telle protectrice des libertés individuelles, elle l'est dans le cadre du contrôle d'une mesure prise par la puissance publique qui est la seule investie d'un pouvoir lui permettant de limiter la liberté de tous.

142. **Le régime d'une mesure de police administrative spéciale**. Les pouvoirs de l'État s'agissant d'une mesure de blocage d'un site sont limités alors que celle-ci doit s'inscrire dans le cadre de la mise en œuvre d'une police administrative spéciale. Le pouvoir administratif est habilité par le législateur à prendre une telle mesure qui procède du régime de règlementation d'une activité définie ou qui considère la protection de l'ordre public s'agissant d'un trouble spécialement défini.

Actuellement le blocage d'un site s'envisage dans le cadre de la police des jeux d'argent et de hasard en ligne. L'article 61 de la loi n°2010-456 « *relative à l'ouverture de la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne* » permet au président de l'ARJEL de saisir le président du TGI de Paris pour qu'il fasse ordonner en référé, auprès des FAI, le blocage d'un site de jeu qui se serait soustrait à la procédure d'agrément. Par ailleurs l'article 6-1 de la LCEN organise le blocage des sites qui diffusent des images ou des représentations de mineurs relevant de l'article 227-23 du CP, c'est-à-dire à caractère pédopornographique, et des sites dont le contenu réalise l'infraction de l'article 421-2-5 du CP qui incrimine la provocation à des actes de terrorisme ou l'apologie de tels actes.

Ainsi le respect des libertés individuelles est contrôlé par le Conseil constitutionnel qui peut être saisi de la loi instituant un tel pouvoir de police administrative, et qui de fait ne l'a pas censurée alors qu'il ne s'agit que d'une restriction à l'accès à des services de communication au public et non une privation de l'accès au réseau en lui-même. De plus les décrets d'application de telles mesures peuvent faire l'objet d'un recours pour excès de pouvoir. Enfin une personnalité qualifiée, désignée au sein de la CNIL, s'assure de la régularité des demandes de retrait décidées par l'Office Central de Lutte Contre la Criminalité liée aux technologies de l'information et de la Communication (OCLCTIC).

Assurés d'un régime garant de leur liberté de naviguer s'agissant des mesures de blocage de sites, les internautes peuvent toutefois se voir restreindre l'accès à certains sites et services du web qui peuvent être réservés à une audience spécifiée.

Chapitre 2ème : La règlementation des limitations à la consultation de certains sites et services

143. **La règlementation des limitations possibles à la consultation de certains sites et services.** La liberté de naviguer consiste en la possibilité d'atteindre tous les points du réseau. Elle se réalise par l'abstention, par principe, de l'État au niveau de l'acheminement des connexions ; les pouvoirs publics étant toutefois fondés à la mise en œuvre de mesures de blocage de sites dans le cadre de polices administratives spéciales. Cette gouvernance de la structure établie, il faut envisager d'une part, que le principe est alors que l'internaute puisse consulter librement tous les sites et services disponibles ; ce qui ne veut pas dire évidemment que tous les contenus puissent être mis en ligne.

Or apparaît ici le pouvoir des moteurs de recherche, qui, aujourd'hui sont l'interface indispensable entre l'internaute et les ressources existantes. Grâce à leurs algorithmes, ils orientent l'internaute et il faut considérer dans quelle mesure leurs pratiques peuvent être encadrées (**Section I)**. Par ailleurs, ce principe de liberté de consultation n'exclut pas que l'accès à certains sites et services soient interdits à certains publics, mais alors il faut veiller à la légalité de cette discrimination dans le cadre de politiques publiques définies **(Section II)**.

Section I. L'encadrement de l'activité des moteurs de recherche

144. **Le rôle d'un moteur de recherche dans la mise en œuvre de la liberté de naviguer sur le web**. Le rôle d'un moteur de recherche s'agissant de la mise en œuvre de la liberté de naviguer sur le web est essentiel. En effet un internaute ne peut atteindre des sites et services du web que s'il est correctement aiguillé vers toutes ces ressources. La fonction d'un moteur de recherche apparaît qui n'est pas de fournir un accès aux points du réseau mais d'organiser la publicité des ressources mises en ligne sur celui-ci.

Ainsi il est important, à titre préliminaire, d'indiquer que si un lien est retiré ou rétrogradé de la liste des résultats, l'accès au site n'est pas condamné alors que celui-ci est toujours en ligne. Il a aussi été souligné qu'un moteur de recherche ne peut être exhaustif dans les liens qu'il présente et qu'il n'est pas un mode de recherche exclusif de

l'information[333]. Le Conseil de la concurrence oppose dès lors, en l'an 2000, à une requérante qui s'estimait lésée dans la publicité faite à son site web par le moteur de recherche de *Google*, que : «*la fonction d'annuaire de recherche ou moteur de recherche sur Internet ne peut être tenue pour indispensable à la rencontre de la demande émanant du consommateur et l'offre de produits et services vendus sur Internet* » [334] ; et le Conseil de préciser que l'internaute peut directement taper l'adresse du site dans son navigateur. Une position déjà critiquée en l'an 2000 et qui est difficilement recevable aujourd'hui eu égard à la généralisation de la recherche par mots-clefs via des moteurs de recherche. Ainsi inversement, en 2013, le juge des référés français, amené à se prononcer sur des mesures visant le déréférencement d'un lien vers un site de streaming[335], soutient à l'inverse que : « *En effet, sans l'extrême facilité dans la recherche d'une quelconque information et notamment toutes celles relatives aux sites en cause, l'internaute amateur risquerait d'être découragé s'il devait lui-même frapper le nom de domaine voire l'URL lui permettant d'accéder aux sites susvisés »*[336].

La problématique n'est pas celle d'autres moyens d'accès à la ressource ; elle est celle de l'orientation de l'internaute qui utilise un moteur. La question est alors de savoir dans quelle mesure une telle activité peut être encadrée par l'État pour que soit garantie sa liberté de naviguer. En effet l'internaute ne peut être arbitrairement orienté vers certains liens favorisés dans la liste de résultats, ni privé de certains autres qui auraient été déréférencés. Ainsi il est légitime de s'interroger sur la mise en œuvre de l'algorithme d'un moteur de recherche et sur les conditions du déréférencement de certains liens.

145. ***Plan***. Or il sera vu dans un premier temps que la liberté d'entreprendre des moteurs de recherche doit être respectée, ce qui ne veut pas dire que leur activité ne peut être régulée **(§1).** Dans un second temps il sera démontré dans quelles mesures les actions visant le

[333] V. MANARA C., « La « search neutrality » : mythe ou réalité ? », *Concurrences*, N°1-2011, Doctrines, p.53.

[334] Décision du Conseil de la concurrence n°00-D-3é du 9 juin 2000 relative à une saisine au fond et une demande de mesures conservatoires présentées par la société Concurrence : BOCC, 25 juill. 2000, p.422. V : G.DECOCQ, « Première rencontre entre le droit de la concurrence et les pratiques en matière de nommage et de recherche de site », *CCE* 2000, n°11, comm., n°119 et C.MANARA, « Exercice d'une activité de commerce électronique : accession au domaine « .fr » et ententes », *D*. 2000, AJ, p. 391.

[335] Sur le fondement de l'article L336-2 du CPI.

[336] TGI Paris, ord. réf., 28 nov. 2013, APC et al c/Auchan Télécom et al.

On peut également dénoncer à cet endroit à nouveau les pratiques des régimes autoritaires qui restreignent d'une manière telle cette liberté de consultation qu'ils la vident de sa substance. Par exemple la Chine ne se contente pas d'agir sur les points du réseau accessibles, elle contraint également les choix de connexions de ses résidents en filtrant par mots-clefs leurs requêtes, que ce soit au niveau de l'URL renseigné dans la barre d'adresses ou même au niveau des pages de résultats d'un moteur de recherche[336]. Il faut condamner la mise en œuvre d'un procédé de filtrage par mots-clefs des sites et ressources à disposition sur le réseau alors que ce mécanisme de par sa généralité et son imprécision vide de sa substance la liberté de consulter tous les sites et services du Web.

déréférencement d'un lien menant à un site web sont envisageables, alors que celles-ci ne peuvent se substituer au régime visant les mesures administratives de blocage des sites mis en ligne **(§2).**

§1) Le respect de la liberté d'entreprendre des moteurs de recherche

146. **La problématique du contrôle de l'activité d'un moteur de recherche par les pouvoirs publics**. Lors d'une conférence sur « *Les enjeux juridiques européens autour de l'agenda numérique 2020* », un député européen s'exclamait « *Si Google avait été français, nous l'aurions nationalisé* !»[337]. Derrière cette formule, apparaît l'enjeu de service public d'un moteur de recherche qui est l'interface indispensable à la navigation sur le web. Entre l'internaute, qui dispose d'une connexion au réseau, et les ressources du web, il est un nouvel acteur qui intervient : le moteur de recherche. Disant cela, est ressentie l'exigence d'une garantie s'agissant du traitement de la demande de l'internaute sans qu'apparaisse clairement le sens à donner à celle-ci. En effet le raisonnement autour d'un principe de neutralité qui, affirmé de manière générale, était déjà était peu pertinent au regard des opérateurs de communications, l'est encore moins s'agissant d'un moteur de recherche.

Ainsi il ne s'agit pas d'imposer un principe de neutralité qui n'a aucun sens eu égard à une activité, qui par essence, ordonne les informations. **(A).** Toutefois cette activité doit être régulée alors qu'évidemment une entreprise de moteur de recherche ne peut en dehors de tout cadre défini favoriser ses propres ressources **(B).**

A] L'impossible neutralité d'un moteur de recherche

147. **Le nécessaire classement des ressources.** En l'an 2000, une requérante arguait devant le Conseil de la concurrence que les utilisateurs d'un moteur de recherche étaient « *doublement trompés* » puisque, d'une part, ils n'étaient pas informés des critères de tri des résultats et que d'autres part ces critères, par le biais des « méta-tags », pouvaient être falsifiés ou orientés[338]. Deux problématiques sont dissociées : d'une part celle du secret attaché à l'algorithme et d'autre part celle d'une pratique anticoncurrentielle dans la mise en œuvre de celui-ci. La difficulté est qu'en réalité les deux questions se superposent : le secret du procédé fait peser des doutes sur le respect de la concurrence par *Google*, le moteur visé en l'espèce.

[337] V. les propos introductifs de Jean Lamassoure, député européen, Président de la Commission spéciale taxe, lors de la journée du 7ème forum de *TransEuropeExperts*, lundi 21 mars 2016.

[338] Décision du Conseil de la concurrence n°00-D-31 du 9 juin 2000 relative à une saisine au fond et une demande de mesures conservatoires présentées par la société Concurrence : BOCC, 25 juill. 2000, p.422. V : G.DECOCQ, « Première rencontre entre le droit de la concurrence et les pratiques en matière de nommage et de recherche de site », *CCE* 2000, n°11, comm., n°119 et C.MANARA, « Exercice d'une activité de commerce électronique : accession au domaine « .fr » et ententes », *D*. 2000, AJ, p. 391.

Or il ne saurait être reproché à *Google* de ne pas révéler la teneur de son algorithme. Celui-ci réalise son savoir-faire et l'actif de son entreprise s'agissant de cette activité historique de classement et il peut être considéré comme un véritable secret industriel[339].

Cela dit, il est légitime de s'interroger sur l'objectivité du classement. Un choix est fait puisque nécessairement il faut classer les résultats ; celui-ci répond d'une logique discriminante puisque il est mis en œuvre par un algorithme. A cet endroit le terme de neutralité n'a aucun sens. Comme le dit parfaitement Cédric Manara : le biais est inhérent au service même[340]. Il ne peut être de « *search neutrality* » ; obligatoirement un résultat sera placé en tête et seulement quelques liens apparaîtront sur la première page au regard des mots-clefs tapés. Toutefois il faut considérer que la discrimination opérée par l'algorithme n'est pas subjective puisque la logique même du service, qui est commercial, est d'établir un classement pertinent au regard des attentes des consommateurs.

148. **Les limites à la liberté éditoriale du moteur de recherche.** Utilisant la formule de liberté éditoriale, Cédric Manara souligne les limites de celle-ci : « *Cette liberté se conjugue en effet avec un risque économique pour ces acteurs de l'organisation de l'information, qui fournissent des résultats d'après leurs estimations de ce que les utilisateurs jugeront pertinent […]. C'est sur la base de la qualité de service fourni que ces derniers décideront de les utiliser à nouveau ou non. En conséquence, les contraintes de marché des moteurs de recherche ont pour effet de limiter en pratique leur liberté éditoriale, qui peut difficilement être comprise comme un discrétion absolue dans la façon de ranger les résultats »*[341]. Ainsi la logique même du classement des ressources, qui répond de celle d'un service commercial, obéit à une dynamique qui ménage une visibilité cohérente et concurrentielle des liens. Cette dynamique, sans que l'algorithme soit dévoilé, peut être concrètement appréhendée ce qui permet à chacun de travailler à un meilleur référencement de son site web, et inversement à *Google* de sanctionner toute activité qui chercherait à tromper les algorithmes[342].

Cela dit, la seconde problématique se pose, et le raisonnement limpide de Cédric Manara peut être repris : « *Réguler la neutralité paraît un non-sens car la neutralité ne*

[339] V. MANARA C., « La « search neutrality » : mythe ou réalité ? », *Concurrences*, N°1-2011, Doctrines, p.55.
[340] V. MANARA C., « La « search neutrality » : mythe ou réalité ? », *Concurrences*, N°1-2011, Doctrines, p.55.
[341] MANARA C., *op.cit*, p.54.
[342]DEMPURE F., « Le classement des sites par les moteurs de recherche », *JCP G.*, n°10-11, 10 mars 2014, Tendances, p.326

peut exister en l'espèce. En revanche des préoccupations de concurrence pourraient-elles naître à raisons des résultats fournis par les moteurs ? »[343]. Il faut répondre par l'affirmative et envisager le contenu de la régulation de l'activité d'un moteur de recherche.

B] La régulation de l'activité d'un moteur de recherche

149. ***Plan.*** Aujourd'hui l'exigence de neutralité des moteurs de recherche s'envisage à travers un principe de « loyauté des plateformes », introduit en France par la loi pour une République numérique **(1).** Si ce dernier dessine les contours d'un régime d'information auprès du consommateur s'agissant du fonctionnement de ces activités de classement de liens et de services, le contrôle de la mise en œuvre même de l'algorithme doit s'envisager à travers les règles du droit de la concurrence **(2).**

1) Le principe de « loyauté des plateformes ».

150. **Le principe de loyauté des plateformes.** La formule de neutralité des moteurs de recherche a été abandonnée ; elle a été remplacée par un principe de « *loyauté des plateformes* »[344], dont « *l'anthropomorphisme exacerbé* »[345] est toutefois maladroit.

Ce principe vise à encadrer « *les risques de biais et de manipulation* »[346]de la part de ces services dit d'intermédiation qui sont définis à l'article L111-7 du Code de la consommation comme : « *toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; 2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service.* ».

Le II de l'article poursuit en indiquant que tout opérateur est tenu de délivrer au consommateur une information loyale, claire et transparente sur : « 1° *Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ; 2° L'existence d'une relation*

[343] MANARA C., *op.cit*, p.55.

[344] V. : Titre II : « La protection des droits dans la société numérique », Chapitre 1er « Environnement ouvert », Section 3 : « Loyauté des plateformes et information des consommateurs », Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, (JORF du 8 octobre 2016, Texte 1 sur 96).

[345] J.ROCHFELD et C. ZOLYNSKI, « La « Loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT*, novembre 2016, p.522.

[346] *Ibid.*

contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne ; 3° La qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale, lorsque des consommateurs sont mis en relation avec des professionnels ou des non-professionnels. ».

Toutefois cette obligation d'information de leurs pratiques à l'égard des consommateurs ne peut se confondre avec une transparence de l'algorithme et cette loyauté est limitée.

151. **Les limites de ce régime.** Sans revenir sur les hésitations qui pèsent sur cette *« méta-qualification* »[347] visant les plateformes qui, de fait, s'agissant d'un service de moteur de recherche généraliste, s'applique ici, le contenu de cette obligation de « loyauté »est incertain.

Les professeures Judith Rochfeld et Célia Zolynski soulignent ainsi la limite matérielle de cette obligation et regrettent que l'exigence de loyauté ne porte pas également sur les algorithmes citant la « *gouvernementalité algorithmique* »[348] qui nous saisit. Elles s'interrogent sur un référencement ou une présentation qui serait plus « neutre ». Par ailleurs, elles relèvent que la loyauté n'intervient qu'entre le consommateur, l'internaute donc, et la plateforme et qu'elle ne concerne pas «*l'autre face de l'intermédiation, c'est-à-dire des utilisateurs professionnels, fournisseurs de « contenus* » »[349]. Il n'est pas d'obligation d'information dans le cadre de ces rapports dit de « BtoB » pour « *Business-to-Business* ». Elles concluent l'analyse de ce nouveau régime en citant l'article L111-7-1 du Code de la consommation qui oblige, à partir d'un certain seuil de connexions, à la diffusion de bonnes pratiques auprès des utilisateurs qui seront contrôlées par une autorité administrative compétente. C'est donc une « *régulation réputationnelle* »[350] qui selon leur formule se trouve promue. Comme il est justement affirmé : « *La loyauté est ainsi appelée à devenir un argument de marketing en tant que facteur de différenciation converti en avantage compétitif »*[351].

[347] J.ROCHFELD et C. ZOLYNSKI, « La « Loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT,* novembre 2016, p. 520.

[348] En référence à l'article de A .ROUVROY et T. BERNS, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux,* 2013/1, n°177, p. 163-196. Cité par J.ROCHFELD et C. ZOLYNSKI, « La « Loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? », *Dalloz IP/IT,* novembre 2016, p.523.

[349] *Ibid.,* p. 523.

[350] *Ibid.,* p. 524.

[351] *Ibid.,* p. 524.

Ainsi la formule très maladroite de loyauté pressent l'enjeu des plateformes à l'égard des internautes s'agissant de leurs accès aux services et informations référencés mais conduit à le formaliser dans une obligation de transparence qui n'a pourtant pas, dans un premier temps, à les concerner. En effet la mise en œuvre d'un algorithme référençant des liens, des services, des informations, oriente sans conteste un choix mais n'aboutit jamais à une décision visant l'individu. Un tel algorithme n'a pas à répondre de garanties de neutralité ou de transparence vis-à-vis de l'individu, puisqu'il ne le discrimine pas ; il discrimine les contenus référencés. En revanche, il faut contrôler tout abus qui préjudicierait non pas l'internaute mais le service qui souhaite être référencé. Ici intervient le droit de la concurrence.

2) L'application du droit de la concurrence

152. **La sanction des abus à la liberté d'entreprendre d'un moteur généraliste tel Google.** A l'endroit de l'algorithme d'un moteur de recherche généraliste tel *Google,* il apparaît que tout abus dans l'ordonnancement des résultats doit être sanctionné. De fait il sera découvert puisque visible à l'endroit des pages de résultats. Ainsi en avril 2015, la Commission européenne a adressé une communication des griefs à Google au sujet du service de comparaison de prix faisant valoir que l'entreprise avait abusé de sa position dominante sur les marchés des services de recherche générale sur l'internet dans l'Espace économique européen (EEE) en favorisant systématiquement son propre comparateur de prix dans ses pages de résultats de recherche générale[352]. Aujourd'hui, alors que Google multiplie les services associés à cette activité d'ordonnancement, les problématiques de concurrence et d'abus de position dominante s'apprécient à une autre échelle[353].

---

[352] V. le communiqué de presse de la Commission européenne, en date du 15avril 2015, « Abus de position dominante : la Commission adresse une communication des griefs à Google au sujet du service de comparaisons de prix et ouvre une procédure formelle d'examen distincte concernant Android ». Communiqué disponible à cette adresse : http://europa.eu/rapid/press-release_IP-15-4780_fr.htm

[353] Ainsi en avril 2016 la Commission européenne a informé Google de sa conclusion préliminaire selon laquelle la société a, en violation des règles de concurrence de l'UE, abusé de sa position dominante en imposant des restrictions aux fabricants d'appareil Android et aux opérateurs de réseaux mobiles. Elle indique également ses préoccupations concernant la copie de contenus web concurrents (connue sous le nom de « scraping » ou « moissonnage »), l'exclusivité en matière publicitaire et les restrictions injustifiées imposées aux annonceurs. (V. : le communiqué de presse de la Commission européenne sur ce point en date du 20 avril 2016).

En France, dans le cas du contentieux du marché de la cartographie qui voyait les sociétés Google France et Google Inc attaquées par la société Evermaps, anciennement Bottin Cartographes pour la mise en œuvre gratuite de l'application « google Maps », la CA de Paris le 25 novembre 2015 a réformé le jugement de 1ère instance et considéré qu'il n'y avait pas de pratique de prédation, v. DECOCQ G. « Google n'a pas eu de stratégie d'éviction sur le marché de la cartographie », *CCC,* janvier 2016, comm. n°19.

V. également : BOSCO D. « GAFA et droit de la concurrence », *CCC,* avril 2016, repère n°4. V. aussi le compte-rendu de l'atelier de droit économique, de l'Institut de Droit des Affaire de la faculté d'Aix-Marseille qui s'est tenu le 28 janvier 2016, et qui est disponible en ligne sur le site ida-aixmarseille.Fr. La professeure Anne-Sophie Choné-Grimaldi a estimé que la caractérisation d'un comportement qui « *dépasse les limites d'une concurrence normale* » dans le cas de *Google* était discutable dès lors que pouvaient être différenciées les entreprises dont la situation de dominance est l'héritage d'un ancien monopole d'État et les entreprises ayant acquis cette position du fait de leurs mérites, en proposant de meilleurs produits et services.

Ainsi cette étude considère que la dynamique technique et commerciale de l'algorithme du moteur de recherche Google ménage, s'agissant de l'ensemble des ressources du web, un classement efficace et le présupposé ne peut être qu'il est biaisé par des choix subjectifs de l'entreprise Californienne. C'est à l'inverse la logique d'une action délibérée sur le retrait d'un lien vers un site web qui doit être condamnée.

§2) Les conditions du déréférencement d'un site du web

153. **L'action de déréférencer un lien vers un site du web et non un contenu.** Si le lien vers un site est retiré d'un moteur de recherche généraliste tel Google, l'internaute qui a l'habitude d'être dirigé sur le réseau en tapant des mots-clefs dans le moteur et en cliquant sur les liens affichés est perdu. Il est lui est difficile, seul, de retrouver le chemin pour accéder au site web désiré. Or cette action sur l'accès même à un site du web via son déréférencement peut s'apparenter à un blocage du site.

Toutefois, il faut être précis sur l'action de déréférencement envisagée ici : il n'est question en l'espèce que du régime de déréférencement d'un lien menant à un site web et non du déréférencement d'un contenu comme une image ou une vidéo. La problématique du retrait des liens apparaissant à la saisie des nom et prénom d'un individu dans la barre de recherche n'est pas non plus traitée. En effet, le lien vers une page de site contenant une information sur l'individu n'est pas déréférencé de manière générale mais l'est seulement au regard des nom et prénom de l'individu choisis comme mots-clefs. La problématique du droit à l'oubli n'a pas trait au régime de la liberté de naviguer sur le web mais renvoie à celui de la liberté d'expression et d'information. Toutefois, le raisonnement peut procéder de la même logique : doit être questionnée l'unicité d'un régime visant tout à la fois le déréférencement d'une photo ou d'une vidéo d'un individu et celui d'un lien vers une page web le mentionnant. La réflexion à cet endroit amène à être très réservé sur le sens du contrôle automatique donné à un individu sur ce que l'on dit de lui alors qu'il faudrait d'abord réfléchir aux évolutions des mécanismes d'archivage et du droit de la presse à cet endroit.

Eu égard à la liberté de naviguer sur le web, la problématique est celle du retrait d'un lien vers un site, c'est-à-dire un nom de domaine. L'enjeu en effet est de manière plus efficace, car moins couteuse et plus rapide, de bloquer des sites du web en agissant

---

Défendant la position inverse en faveur d'un abus, Guillaume Grundeler a arguait lui d'un devoir d'objectivité dans le classement des résultats généraux.

directement sur les liens référencés. Or cette politique ne peut être. Comme l'étude l'a montré, toute atteinte à la liberté de naviguer d'un internaute ne peut ressortir que d'un régime d'ordre public.

154. ***Plan.*** Ainsi d'une part, il faut considérer que les pouvoirs publics sont fondés à requérir des moteurs de recherche qu'ils déréférencent des liens vers des sites du web dès lors que ces demandes répondent du même régime que celui visant les mesures de blocage auprès des FAI **(A).** D'autre part, il faut condamner, en revanche, toute action judiciaire qui dans un mimétisme avec celle possible auprès des hébergeurs de contenus, tend à requérir du juge des référés qu'il ordonne le retrait d'un lien vers un site du web **(B)**.

A] L'encadrement de la mesure de déréférencement à l'initiative des pouvoirs publics

155. **Les conditions déréférencement à l'initiative des pouvoirs publics français.** Il apparaît d'abord que les pouvoirs publics sont fondés à mettre en œuvre des mesures de déréférencement qui viennent compléter les mesures de blocage de sites et qui répondent du même régime protecteur s'agissant de la liberté de naviguer de l'internaute.

Ainsi la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions de la lutte contre le terrorisme a permis à l'autorité administrative de demander non seulement aux FAI de bloquer l'accès aux sites provoquant aux actes de terrorisme ou en faisant l'apologie et visant également ceux diffusant des images ou des représentations de mineurs à caractère pornographique, mais également de requérir des moteurs de recherche qu'ils suppriment les liens vers de tels sites de leur liste de résultats[354].

Cette mesure est insérée dans le nouvel article 6-1 de la loi pour la Confiance en l'Économie numérique, au niveau de son alinéa 4 : «*L'autorité administrative peut également notifier les adresses électroniques dont les contenus contreviennent aux articles 421-2-5 et 227-23 du code pénal aux moteurs de recherche ou aux annuaires, lesquels prennent toute mesure utile destinée à faire cesser le référencement du service de communication au public en ligne. La procédure prévue au troisième alinéa du présent article est applicable* ». Ainsi ces mesures sont soumises au contrôle de la personnalité qualifiée. Par ailleurs le décret n° 2015-253 du 4 mars 2015[355] vient préciser cette procédure de déréférencement. Il est rappelé que les moteurs de recherche

[354] V. Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions de la lutte contre le terrorisme+. Chapitre V « *Renforcement des moyens de prévention et d'investigations* », article 12

[355] Décret n°2015-253 du 4 mars 2015 « relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique »

préservent la confidentialité des données qui leur sont ainsi confiées[356] et que l'OCLCTIC s'assure chaque trimestre que les adresses qui ont été notifiées et retirées présentent toujours un caractère illicite[357].

De plus dans le cadre du régime de l'activité règlementée des jeux d'argent et de hasard en ligne, l'alinéa 5 de l'article 61 de la loi n°2010-476 « *relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne* » habilite le président de l'ARJEL à saisir le président du tribunal de grande instance de Paris aux fins de prescrire une mesure de déréférencement auprès d'un moteur de recherche ou d'un annuaire.

Ces régimes de polices administratives spéciales, qui circonscrivent les sites visés et définissent une procédure de contrôle et d'actualisation de la mesure mise en œuvre sont garants de notre liberté de naviguer sur le réseau, ce qui n'est pas le cas d'une mesure de retrait de lien à l'initiative d'un particulier quand bien même ordonnée par un juge judiciaire.

B] Le non-sens d'une action en justice visant le déréférencement d'un lien menant à un site web

156. **Le non-sens d'une action en justice visant le déréférencement d'un site du web**. De la même manière que cela a été démontré s'agissant de l'activité des FAI et de leur possibilité de blocage d'un site, il faut affirmer que l'article 6-I-2 de la LCEN ne peut s'appliquer aux moteurs de recherche, qui ne peuvent être sommés par un particulier de retirer un lien vers un site du web après simple notification.

La généralité de cette procédure ne se conçoit que parce que son champ d'action est délimité : un hébergeur, en relation avec un éditeur qu'il doit pouvoir identifier, retire un contenu. Il convient également de condamner tout déréférencement de site en application des mesures spécifiques visant la lutte contre la contrefaçon pouvant être prises sur le fondement de l'article L336-2 du CPI.

En effet l'exemple peut être pris de l'action d'organismes de défense professionnelle qui sur ce fondement ont demandé au juge des référés que soient bloqués et déréférencés des sites de streaming bien connus, tel « *Alloshowtv* », qui réalisaient des actes de contrefaçon[358]. La société *Google* appelée à faire cesser le trouble tente de faire valoir une fin de non recevoir alors qu'elle indique qu'elle a déjà fait droit aux

[356] *Ibid.*, article 3.
[357] *Ibid.*, article 4.
[358] TGI Paris, ord. réf., 28 nov. 2013, *APC et al c/Auchan Télécom et al*. V. : PIGNATARI Olivier, « Blocage et déréférencement de plusieurs sites de streaming : à qui profite le stream ? », *RLDI* 2013, n°3294.

demandes de déréférencement des liens vers ces sites en amont de la procédure de référé[359].

Si cet argument ne conduit pas à éteindre l'action alors que de nouveaux sites sont incriminés, le juge constatant qu'il ne peut être fait droit à la demande d'actualisation du filtrage des demandeurs, indique toutefois que les principaux moteurs de recherche ayant déjà mis en œuvre certaines mesures sollicitées, « *il apparaît possible qu'ils acceptent la modification des demandes, en cas d'évolution attestée par les demandeurs, notamment en raison du changement de noms des sites en cause* ». Il faut condamner cette logique qui voudrait que le déréférencement d'un site puisse s'opérer après simple notification alors pourtant qu'à ce niveau la constatation d'une contrefaçon nécessite une appréciation[360]. Il faut réaffirmer avec force que la répression de la contrefaçon perpétrée en ligne doit être le fait d'une politique étatique qui seule peut impulser son actualisation[361].

Les procédures dites de «retrait après notification » ne peuvent être généralisées au déréférencement de liens menant à des sites. Un contrôle des sites accessibles, via leur déréférencement, sur simple demande des ayants-droit sollicitant à cet endroit la libre-appréciation des entreprises du web[362] méconnait la liberté de naviguer de tous sur le réseau.

Assuré que tous les sites du web sont mis à sa disposition selon un régime transparent, l'internaute peut toutefois se voir interdire l'accès à un site ou service spécifié.

---

[359] A la différence d'autres moteurs de recherche comme celui de la société française GIE Orange qui considère qu'une telle mesure nécessite une décision judiciaire.

[360] Ainsi dans l'affaire prise en exemple, le juge renvoie aux constats des agents assermentés et considère qu'il ne peut y avoir d'effets collatéraux au blocage des sites dès lors que «*Dans ces conditions, si on rapporte le chiffre à l'ensemble des œuvres objets de l'étude, le nombre de ces œuvres serait de 0 sur 48577 liens vers des films et moins de 650 œuvres sur les 72354 liens vers des « séries » ne seraient pas des contrefaçons. Le faible nombre de ces liens vers des œuvres dont les droits ne sont pas discutés permet d'admettre que les mesures ordonnées dans les conditions ci-après fixées n'entraîneront pas de dommage disproportionné, étant observé qu'elles ne constituent pas un obstacle absolu empêchant l'accès aux œuvres qui peuvent être vues par d'autres moyens »* TGI Paris, ord. réf. 28 novembre 2013, *Ibid.*

[361] V. *supra* le Chapitre 1er intitulé « Le régime du blocage d'un site, restriction à la liberté de naviguer », 2) « La problématique de la lutte contre les sites de téléchargement illégal ».

[362] Il peut être noté que la société *Google Inc.* a indiqué dans ses écritures que désormais elle avait retenue comme l'un des critères de classement le nombre de demandes de désindexation par URL, de sorte qu'un « *site ayant fait l'objet de nombreuses demandes de désindexation se verra considéré comme moins pertinent et les pages de ce site encore référencées et non signalées seront automatiquement rétrogradées dans l'ordre d'apparition des résultats de recherche »*[362] (TGI Paris, ord. réf. 28 novembre 2013, *op. cit.*) Il faut questionner ici le sens de cette régulation. Certes l'action n'agit pas sur le référencement même du site mais sur sa rétrogradation dans la liste des résultats ; cela dit il est rare qu'un internaute aille au-delà de la 1ère page affichée par le moteur de recherche.

Section II. Le contenu des politiques visant à limiter la consultation de certains sites

157. **L'encadrement de la consultation et non la sécurisation de la connexion.** Les débats sur la lutte contre la contrefaçon en ligne et plus spécifiquement le téléchargement illégal d'œuvres, qui cristallisent de nombreuses problématiques s'agissant des libertés à protéger sur le réseau, font apparaître un exemple pertinent d'une responsabilisation dévoyée du titulaire du point d'accès au réseau, qui ne peut être tenu de sécuriser son accès.

En effet, en 2009, la loi HADOPI oblige le particulier à « *veiller à ce que cet accès* –son accès au réseau- *ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise* »[363] ; obligation qui renvoie à la mise en œuvre par le titulaire de l'abonnement de « *moyens de sécurisation* » de son accès qui doivent lui être proposés par son FAI[364] et qui font l'objet d'une labellisation décidée par la HADOPI[365]. En cas de négligence caractérisée le titulaire de l'abonnement peut être condamné à une contravention consistant en la suspension de son accès au réseau[366].

Cette systématisation de la responsabilité au niveau du point d'accès du réseau et donc du particulier doit être condamnée. Il est illusoire de considérer que l'automatisme du procédé puisse permettre de prévenir automatiquement toute infraction. De fait, la réalité de la labellisation et de la mise en œuvre dans les foyers français de tels systèmes de sécurisation, témoigne si ce n'est de son caractère autoritaire tout du moins de son

[363] Article L336-3 du Code de la Propriété Intellectuelle (CPI). Il est à noter que l'obligation de surveiller son accès mise à la charge du titulaire de l'abonnement date de la loi DADVSI (Loi n°2006-961 du 1er Août 2006 « *relative au droit d'auteur et aux droits voisins dans la société de l'information* » qui insérait un nouvel article L335-12 dans le Code la Propriété Intellectuelle (CPI)). Cette obligation était toutefois dépourvue de sanctions et son effectivité dès lors s'en trouvait limitée. La loi « Création et Internet » la rend effective alors qu' un mécanisme de recommandations et de sanctions mis en œuvre par la Commission des droits de la Haute Autorité, est prévu pour sanctionner son défaut.

Ainsi il a été paré à la censure du Conseil constitutionnel qui avait rappelé en 2006 que plusieurs sanctions ne pouvaient être rattachées à une même qualification de contrefaçon. La riposte graduée ne sanctionne pas un acte de contrefaçon mais un défaut de surveillance par le titulaire de l'abonnement de son accès à internet, une grossière subtilité largement dénoncée. V. notamment : MACREZ F. et GOSSA Julien, « Surveillance et sécurisation : ce que l'Hadopi rate, à propos de la « petite loi » « Création et Internet » », *RLDI* 2009/50, n°1659, p.80.

[364] V. l'article 6-I-1 al. 2. de la LCEN tel que modifié par la loi « HADOPI 1 ».

[365] V. l'article L331-26 du CPI.

[366] La loi n° 2009-1311 du 28 octobre 2009 « *relative à la protection pénale de la propriété littéraire et artistique sur internet* », loi dite « HADOPI 2 » vient préciser que le manquement à cette obligation de sécurisation ne peut engager la responsabilité pénale de l'intéressé. La sanction de la suspension de l'accès fait dès lors l'objet d'une contravention de la 5ème classe en cas de « négligence caractérisée », v. article L335-7-1 du CPI.

Sur le non-sens dans un État de droit d'une peine contraventionnelle de suspension de l'accès au réseau. V. *supra* le titre I intitulé « *La liberté d'accès au réseau* », le chapitre 2 « *La reconnaissance du caractère fondamental de ce nouveau principe* », section II «*Les conditions de la privation d'accès au réseau*».

ineffectivité[367]. La contrainte de la régulation du réseau ne peut peser sur l'individu mais doit ressortir d'un encadrement mis en œuvre par l'État.

Ainsi on ne saurait exiger de sécuriser un accès ; en revanche des conditions d'accès à certains sites peuvent être définies par les pouvoirs publics qui toutefois ne peuvent pénaliser la consultation en soi d'un contenu en dehors de celui réalisant un délit de pédopornographie.

158. ***Plan.*** La règlementation des conditions de consultation de certains sites et services obéit à des politiques publiques éprouvées ; elle est ainsi efficace **(§1).** Il est critiquable en revanche de multiplier les délits de consultation de sites ; un tel régime répressif généralise une surveillance de l'individu qui ne saurait être **(§2)**.

§1) Les conditions de la limitation de l'audience d'un site ou service du web

159. ***Plan.*** Alors que l'internaute peut être empêché d'accéder à certains sites et services du web du fait de sa nationalité, il a été décidé d'encadrer dans l'Union européenne cette pratique dite de « blocage géographique » qui enserre la liberté de naviguer de l'internaute dans les limites de services nationaux **(A).** D'autre part l'accès à certains services du web est aujourd'hui interdit aux mineurs ; toutefois il ne peut être de police administrative visant leur protection à l'échelle de l'ensemble des services du web **(B).**

A] L'interdiction de la pratique dite du « blocage géographique » dans l'Union européenne

[367] Si un décret est venu préciser en 2010 les conditions de labellisation des offres culturelles légales sur le réseau, celui-ci ne vise pas les moyens de sécurisation –Décret n°2010-1366 « *relatif à la labellisation des offres des services de communication au public en ligne et à la régulation des mesures techniques de protection et d'identification des œuvres et des objets protégés par le droit d'auteur* ». Cette labellisation ne fait pas par ailleurs l'objet d'une communication détaillée sur le site de la HADOPI, qui se contente de rappeler l'obligation du CPI sans fournir de lien vers une liste de sites labellisés qui permettrait de faciliter la mise en œuvre concrète de cette obligation par le citoyen, v. le site : www.hadopi.fr. Sur la difficulté d'une technologie totalement efficace, v. MACREZ F. et GOSSA J. « Surveillance et sécurisation : ce que l'Hadopi rate, à propos de la « petite loi Création et Internet », *RLDI* 2009/50, p.79-91

Il est à noter qu'en Allemagne une obligation de surveillance spécifique n'a pas été créée mais que la responsabilité du titulaire de la connexion peut être engagée sur la notion de droit commun qui qualifie l'individu de « *störer* », c'est-à-dire que sans être lui-même auteur ou complice, l'individu a volontairement rendu possible de quelque manière que ce soit le dommage. Plus utilement que ne le fait en France une discussion sur une obligation nouvelle de sécurisation de l'accès, les juges allemands adoptent donc une approche *in concreto* des conditions de la responsabilité. Ainsi dans une espèce où la mise à disposition de fichiers illégaux réalisant une contrefaçon étaient mis à disposition par le beau-fils du titulaire de l'abonnement, la Cour fédérale allemande affirme que la notion de « *störer* » ne peut ici être retenue alors qu'il existe un lien familial et que l'auteur de la contrefaçon est majeur. Dès lors, en l'espèce, ce n'est que si le titulaire a des indices qu'une telle contrefaçon est commise qu'il doit alors prendre les mesures nécessaires pour faire cesser ces actes illégaux. De la même manière plus utilement à l'échelle de la sanction, l'approche allemande met à la charge du titulaire de la connexion l'identification du véritable contrefacteur et la cessation du trouble avant toute sanction pécuniaire. V. BHG, 1ère ch. Civ., 8 janvier 2014, *BearShare*. LEMIEUX T. « La responsabilité de l'abonné internet en cas de contrefaçon en ligne, regard français sur l'affaire *BearShare* », *RLDI*, 2014/109, p. 17-22,3600.

160. ***Plan.*** La pratique dite du « blocage géographique » empêche l'accès à un service ou modifie les modalités de celui-ci en fonction de la nationalité de l'internaute **(1).** Un règlement européen a été adopté le 28 février 2018 visant à contrer ce blocage non pas de manière générale mais quand il est injustifié **(2).**

1) Les enjeux de la pratique dite du « blocage géographique »

161. **La logique technique d'une telle pratique.** La pratique dite du « blocage géographique » ou *« geo-blocking* » considère la nationalité de l'internaute, plus précisément l'indication géographique inhérente à son adresse IP, pour établir les conditions d'accès au service du web demandé.

En effet, la répartition des adresses IP obéit à une logique géographique. A l'échelle du réseau qui est mondial, l'ensemble des connexions opérées au même moment doivent toutes disposer d'un numéro unique, il faut donc organiser une répartition de ces numéros, à cette échelle, selon des règles intangibles qui doivent obéir à un système de publicité. Ce système est mis en œuvre par l'ICANN pour« *Internet Corporation for Assigned Names and Number »,* une organisation internationale sans but lucratif créée aux Etats-Unis en 1998. Or sans entrer dans le détail de la technique d'adressage, celle-ci suit une logique de maillage du territoire.

Ainsi les adresses sont d'abord allouées aux différents registres régionaux d'adresses internet[368]. Cette répartition suit la division opérée par le premier nombre de l'adresse IP ; un tableau de concordance s'établit alors entre le 1er nombre de l'adresse IP et la zone géographique concernée. Ce tableau est public et facilement accessible en ligne[369]. Une adresse IP est nécessairement liée à une zone géographique. Puis les registres régionaux d'adresses internet (RIR de l'anglais *Regional Internet Registry*) distribuent à leur tour les adresses qui leur ont été attribuées, à des registres locaux (LIR de l'anglais *Local Internet Registry*), qui les attribuent ensuite aux opérateurs de communications électroniques nationaux. Cette répartition est publique. Une adresse IP est donc nécessairement liée à un opérateur national qui l'attribue à un point du réseau du territoire national.

[368] Ce sont : l'AfriNIC (Afrique), APNIC (Asie - Pacifique), ARIN (Amérique du Nord), LACNIC (Amérique Latine et Caraïbes) et RIPE NCC (Europe)Voir le site internet de Patrick MAIGRON, enseignant à l'INT sud Paris : « Le tour du net en questions », http://www-public.it-sudparis.eu/~maigron/Internet/, rubrique « Adresses IP », qui est d'une grande clarté pour tous, informaticiens ou non, en ce qui concerne l'adressage du réseau.

[369]Ainsi 32 plages d'adresses IP ont été attribuées au registre européen : 002, 005, 031, 037, 046, 062, 077 à 095, 109, 176, 178, 185, 193 à 195, 212, 213. Par exemple, une adresse IP commençant par 213 renverra nécessairement à un serveur connecté en Europe. V. : http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

Ainsi il faut bien souligner que l'indication géographique est technique et ne renseigne pas sur la nationalité de l'internaute mais sur son lieu de connexion. Disant cela, il faut indiquer à titre liminaire que la pratique qui discrimine la connexion en fonction de l'adresse IP peut donc être contournée techniquement alors qu'il suffit de rediriger la connexion à travers un autre point à la nationalité adéquate[370]. Toutefois ce procédé doit être envisagé comme un procédé dévoyant le mécanisme d'adressage du réseau et à ce titre condamné[371].

162. **La logique commerciale d'une telle pratique.** L'exemple de blocage géographique le plus connu car mis en œuvre de manière transparente est celui des chaînes de télévision s'agissant de leurs services de « *Replay* » ou télévision de rattrapage. En effet en considération des droits de diffusion qu'elles sont en droit d'attendre de la vente à l'étranger de leurs productions audiovisuelles, ces dernières restreignent légitimement l'accès à de tels services disponibles via le réseau internet. Ainsi si un internaute se connecte à partir d'un point de connexion français, il ne peut accéder aux services de *replay* de la chaîne américaine ABC par exemple.

Par ailleurs, le blocage géographique apparaît également s'agissant de services de vente en ligne. L'exemple peut être pris d'une entreprise de location de voitures qui voyant que la demande de location émane d'un pays membre autre que le sien facture plus cher le service comparé à la même demande effectuée depuis le territoire national. De la même manière, la tarification d'une commande en elle-même et non des frais d'envoi proprement dit, est parfois plus élevée quand la demande est faite depuis un pays voisin.

163. **La problématique à l'échelle de l'Europe : la nécessaire réalisation d'un marché unique numérique**. Cette logique de diffusion des contenus montre ces limites alors que la nationalité du point d'accès ne renseigne pas sur la nationalité de l'internaute. Dans le cas d'un service payant par exemple, un national peut légitimement s'attendre à pouvoir accéder à un contenu alors même qu'il se trouve à l'étranger. Or, un internaute français abonné à Canal+ par exemple voit sa connexion à son compte d'accès aux contenus en ligne bloquée

[370] La tendance ces dernières années est à l'utilisation d'un VPN pour *Virtual Private Network*. Il s'agit de connecter des ordinateurs distants en créant virtuellement un réseau local, dès lors l'adressage n'obéit plus à la logique de l'adressage international et permet de passer outre les pare-feux et proxys qui pourraient à l'échelle mondiale restreindre l'accès à des serveurs distants. Récemment cette technique souffre des limites alors que les services de diffusion de contenus ont trouvé des parades mais qui ne sauraient résister longtemps

[371] V. *infra* : Partie 2ème, titre I, chapitre 2ème, Section I, §1 « *Le respect du mécanisme d'adressage du réseau* ».

selon sa position géographique[372]. La problématique peut s'étendre aux contenus des chaînes financées par la redevance ; un national ne peut aujourd'hui profiter de pluzz.fr sur l'application dédiée s'il se trouve à l'étranger.

Dans un communiqué de presse intitulé « Un marché unique numérique pour l'Europe: la Commission définit 16 initiatives pour en faire une réalité », le président de la Commission européenne Jean-Claude Juncker, en 2015, constate ainsi que : « On *peut aller de Tallinn à Toulon en voiture sans montrer une seule fois son passeport mais une fois arrivé là-bas on ne peut pas regarder les émissions de télévision préférées de son propre pays* »[373]. Dès lors la Commission propose de donner « *un caractère moderne et plus européen à la législation sur le droit d'auteur* »[374] pour élargir l'accès au contenu culturel en Europe ce qui favoriserait la diversité culturelle. La Commission souligne par ailleurs la nécessité de réexaminer le cadre des médias audiovisuels qui doit prendre en compte les nouveaux modèles économiques de diffusion de contenus.

De plus, le président de la Commission européenne souligne que les PME européennes ont encore du mal à intégrer le marché du numérique. Il convient donc d'harmoniser les pratiques. Jean-Claude Juncker affirme ainsi, que de la même manière qu'ont été abolies les frontières dans le monde physique par la réalisation d'un marché commun invitant au développement d'une liberté de circulation des citoyens de l'Union, la règlementation européenne doit viser la réalisation d'un *« marché unique numérique* »[375] assurant la liberté de naviguer sur le web des citoyens de l'Union. En 2018, un règlement européen a été adopté en ce sens.

2) Le règlement (UE) 2018/302 visant à contrer le blocage géographique injustifié

164. **Le champ d'application limité du règlement : les services de commerce électronique.** Le règlement (UE) 2018/302 du 28 février 2018 vise « *à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu*

[372] L'on peut s'étonner de cette limitation géographique alors que les conditions d'accès à ce type de compte ont évolué. En effet, l'accès est désormais numériquement limité en fonction du nombre d'écrans, c'est-à-dire en fonction du nombre d'appareils pouvant se connecter en même temps au compte personnel de l'abonné. Voir les offres multi-écrans de *Canal+* et *CanalSat*. Deux téléviseurs et deux appareils tels une tablette ou un Pc peuvent être connectés en même temps. Cinq appareils différents peuvent être connectés sur les dernières 72 heures.

[373] V. la vidéo du communiqué disponible à cette adresse ; http://europa.eu/rapid/press-release_IP-15-4919_fr.htm

[374] *Ibid.*

[375] *Ibid.* Le président de la Commission, Jean-Claude Juncker affirme que sa première priorité est de réaliser un « *fully digital single market* ».

de résidence ou le lieu d'établissement des clients dans le marché intérieur »[376]. Il est applicable depuis le 3 décembre 2018.

Il a pour champ d'application uniquement les sites web de commerce électronique. Sont exclus du champ d'application les services proposant l'utilisation ou la vente de contenus protégés par le droit d'auteur comme les services d'écoute de musique en ligne, ou de livres électroniques, ou encore ceux proposant des logiciels et jeux en ligne. Le Conseil de l'Union européenne précise toutefois dans son communiqué de presse que : « *cette exclusion sera réexaminée par la Commission* »[377]. Par ailleurs d'autres services visés spécifiquement par la directive « services » sont exclus, notamment les services audiovisuels[378].

Ainsi le règlement vise la protection des consommateurs en relation avec des entreprises du web dans le cadre de l'échange de biens ou de services**,** autres que ceux protégés par le droit d'auteur.

165. **La non-discrimination en matière d'accès aux sites web de commerce électronique.** Il condamne les discriminations injustifiées fondées sur la localisation géographique des consommateurs. Les considérants 18 à 21 et l'article 3 du règlement intéressent notre étude alors qu'est spécialement envisagé l' « *accès aux interfaces en ligne* » qui sont définies comme : « *tout logiciel, y compris un site internet, ou une section de site internet, et des applications, notamment des applications mobiles, exploité par un professionnel ou pour son compte et permettant aux clients d'accéder aux biens ou aux services qu'il propose en vue de réaliser une transaction portant sur ces biens ou services* »[379].

Ainsi il est prescrit à l'article 3, 1. qu'« *un professionnel ne bloque ni ne limite, par l'utilisation de mesures technologiques ou autres, l'accès d'un client à l'interface en ligne du professionnel pour des motifs liés à la nationalité, au lieu de résidence ou au lieu d'établissement du client.* ». D'autre part, le 2. de ce même article précise que sans bloquer l'accès au site, le professionnel ne peut pas non plus rediriger l'internaute en raison de ces mêmes motifs géographiques vers une version de l'interface différente de

[376] Règlement (UE) 2018/302 du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n°2006/2004 et UE 2017/2394 et la directive 2009/22/CE, JOUE, 2.3.2018, I.60/1-15.

[377] Conseil de l'Union européenne, communiqué de presse du 27 février 2018, « Blocage géographique : le Conseil adopte un règlement visant à supprimer les obstacles au commerce électronique », disponible sur le site du Conseil européen et du Conseil de l'Union européenne, www.consilium.europa.eu/fr

[378] Article 1er « Objet et champ d'application », Règlement (UE) 2018/302 du 28 février 2018, *op. cit.*

[379] Article 2 « Définition », 16), Règlement (UE) 2018/302 du 28 février 2018, *op. cit.*

celle à laquelle le client a voulu accéder, « *sauf si le client a expressément donné son consentement à cet effet* ». Et il est bien indiqué que même en cas d'acceptation d'une version spécifique à sa nationalité, le client redirigé doit toujours avoir la possibilité d'accéder facilement à l'interface qu'il avait initialement requise.

Le troisième point de l'article 3 énonce cependant que ces interdictions ne sont pas applicables si le blocage ou la redirection relève d'une exigence légale du droit de l'Union ou d'une législation nationale conforme au droit de l'Union. Cependant le consommateur doit toujours être informé de manière claire et spécifique par le professionnel des raisons de ce blocage ou de cette limitation d'accès.

Ainsi un régime protecteur de la liberté de naviguer est mis en œuvre s'agissant des pratiques de blocage géographique visant l'accès à un site du web qui peuvent obéir à un régime légal ; mais ces pratiques doivent être condamnées si elles sont mises en œuvre par le professionnel en dehors de celui-ci de manière injustifiée. S'il ne peut y avoir de discrimination par la nationalité pour restreindre l'accès à un site web, en revanche l'âge de l'internaute peut être pris en compte pour ce faire.

B] Les limites d'une police administrative spéciale visant la protection des mineurs sur le web

166. **La police administrative spéciale visant la protection des mineurs**. L'internaute agissant sur le web peut être requis de s'identifier pour l'accès à certains services du web. L'objectif des polices mises en œuvre alors n'est pas le respect de l'ordre public envisagé de manière générale mais l'encadrement de certains services du web ou de pratiques qu'il permet, comme l'expression en ligne. Toutefois la limite est ici celle de l'objet d'une police administrative spéciale qui rend légitime cette requête.

Ainsi les pouvoirs publics, dans le cadre de la mise en œuvre de cette police administrative spéciale visant la protection des mineurs, peuvent requérir de certains sites qu'ils s'assurent de l'âge de l'internaute qui souhaite se connecter à leurs services et requièrent dès lors ses documents d'identité En effet la protection des mineurs est un enjeu d'ordre public. Toutefois celle-ci ne peut s'envisager généralement à l'égard de l'ensemble des services du réseau. Cet objectif de protection des mineurs doit se réaliser dans le cadre d'une police administrative spéciale.

Ainsi il est tout à fait envisageable de requérir de l'internaute un document d'identité pour s'assurer de sa majorité dans le cadre de la mise en œuvre d'une activité réglementée **(1).** En revanche il faut s'interroger sur les prescriptions du règlement général sur la protection des données personnelles qui encadre la licéité d'un traitement

de données s'agissant d'un mineur dans le cadre d'une offre de service de la société de l'information. Une prescription notamment à l'usage des réseaux sociaux qui ne peut toutefois relever d'un régime de police administrative spéciale alors que tout site web ne peut en être l'objet. Il ne peut y avoir de contrôle de l'âge de l'internaute s'agissant de tous les services de communication au public en ligne **(2)**.

1) Les dispositions adoptées dans le cadre la régulation d'activités réglementées

167. **L'article 5 de la loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne**. Cet article dans son premier alinéa énonce que les mineurs même émancipés ne peuvent prendre part à des jeux d'argent et de hasard qui sont soumis à une autorisation des pouvoirs publics, à l'exception des jeux de loteries à but non lucratif, des lotos traditionnels et des loteries proposées dans les fêtes foraines.

Son alinéa 2 prescrit alors que « *les opérateurs de jeux d'argent et de hasard légalement autorisés sont tenus de faire obstacle à la participation des mineurs même émancipés, aux activités de jeu ou de pari qu'ils proposent* »[380]. La formulation est claire : il s'agit ici d'une obligation à la charge des opérateurs de jeux. Ainsi dans les faits, les sites de paris en ligne organisent un contrôle de l'identité de l'internaute qui souhaite ouvrir un compte. L'internaute doit produire un document officiel justifiant de son identité et de sa date de naissance. Les sites se prémunissent de toute usurpation de celle-ci en envoyant par voie postale à l'adresse indiquée un code d'activation du compte[381].

Il faut souligner que le législateur français n'a pas expressément requis cette procédure de contrôle d'identité. Elle ressort de la responsabilité des opérateurs. Le dernier alinéa de l'article 5 enjoint *a minima* à ce que la date de naissance d'un joueur soit exigée au moment de son inscription et requise à chacune de ses visites sur le site[382].

[380] Article 5, alinéa 2, de la loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne

[381] V. : les CGU du site *Unibet.fr,* « 3. Modalités d'inscription et de validation du compte, 3.1 Compte provisoire, 3.2 Documents d'identité et compte bancaire, 3.3 Compte d'activation, 3.4 Les délais à respecter » ; les CGU de *Betclic.fr,* « 3. Inscription et ouverture de votre compte », et notamment les points 3.8 et 3.11 qui expliquent que le compte provisoire ne peut se transformer en compte définitif qui si une copie d'un justificatif d'identité est transmise dans les 60 jours suivant l'inscription sur le site ; les CGU du site *PMU.fr,* « Modalités d'ouverture d'un compte joueur » ; les CGU du site *Winamax.fr,* « Article 2. Modalités d'inscription et engagement du joueur ». Toutes ces CGU requièrent l'envoi d'un justificatif d'identité et ne mettent en œuvre un compte définitif que par le biais d'un code d'activation envoyé au domicile de la personne.

[382] Article 5, alinéa 3, de la loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne

168. **L'insuffisance des dispositions du Code de la santé publique s'agissant de la protection des mineurs dans le cadre de la lutte contre l'alcoolisme**. La vente d'alcool en ligne relève du au régime de la vente à emporter des débits de boissons. Le site en ligne doit obtenir une « petite licence à emporter » ou une « licence à emporter » et être déclaré en mairie[383]. Il est donc soumis aux dispositions du Code de la santé publique visant la lutte contre l'alcoolisme et la prévention des mineurs.

Ce code précise dans son article 3342-1 que : « la vente des boissons alcooliques est interdite aux mineurs. L'offre de ces boissons à titre gratuit à des mineurs est également interdite dans les débits de boissons et tous commerces ou lieux publics. La personne qui délivre la boisson exige du client qu'il établisse la preuve de sa majorité. ». Toutefois il faut regretter que cette interdiction n'ait pas fait l'objet de prescriptions spécifiques s'agissant de la vente en ligne. A la différence des sites de jeux d'argent et de hasard en ligne, les opérateurs de sites web ne sont pas visés et il apparait moins évident qu'ils soient tenus de faire obstacle à la vente d'alcool aux mineurs.

Dès lors *a minima*, la plupart des sites font aujourd'hui apparaître la mention que la vente d'alcool est interdite aux mineurs mais exigent simplement que l'internaute connecté déclare être majeur et ce par un simple clic[384]. Cette logique est à condamner. S'agissant d'une activité réglementée comme la vente d'alcool en ligne, il ne s'agit pas de faire peser la responsabilité de la limite d'âge légal sur le consommateur mais bien d'empêcher tout mineur d'acheter de l'alcool. Les formulaires de création de comptes-clients devraient suivre la procédure mise en œuvre par les sites de jeux d'argent en ligne. Le site de commerce en ligne d'alcool doit s'assurer de l'identité de son client.

En revanche, ce contrôle d'identité ne peut être mis en œuvre de manière générale à l'échelle des services de la société de l'information, qui de fait recouvrent les services de commerce électronique.

[383] Article L3331-3 du Code de la Santé publique.

[384] V. : le site Whisky.fr qui fait apparaître dès que l'on s'y connecte un bandeau pop-up qui indique « Bienvenue, Pour accéder à notre site, vous devez avoir plus de 18 ans. Je déclare être majeur et j'accepte les conditions du site ». Il faut alors cliquer sur le bouton « Je déclare être majeur » pour accéder au contenu du site, et le déclarer à nouveau lors de toute commande. Ce bandeau remplit également l'obligation d'information s'agissant des dangers d'une consommation excessive et ce de manière claire.

En revanche, par exemple, il n'est demandé aucune déclaration de majorité sur le site Granitbleu.com qui énonce seulement dans ses « Conditions de vente » que « *L'acheteur reconnaît que la vente de boissons alcoolisées est interdite aux mineurs et s'engage à ne pas passer commande de ce type de produit s'il ne remplit pas cette condition. Le vendeur ne pourra en aucun cas voir sa responsabilité engagée si un client mineur venait à passer outre cette clause.* » et qui a inscrit en bas de sa page d'accueil la mention « *Vente d'alcool strictement interdite aux mineurs* ». De plus on peut noter que la mention « *L'abus d'alcool est dangereux pour la santé* » apparaît sur la page d'accueil du site mais en bas de page et en très petits caractères.

Sur le site coté-aperitif.com, il n'est aucune publicité de la limite d'âge. Il n'est pas requis de déclarer que l'on est majeur. Les conditions générales de vente énoncent seulement que : « *La vente de produits spiritueux et vins de Coté Apéritif est strictement réservée aux personnes désignées comme majeures par leur législation nationale (dix-huit ans pour la France)* ».

2) La limite de l'article 8 du RGPD visant le traitement de données personnelles d'un mineur dans le cadre d'un service de la société de l'information

169. **L'article 8 du RGPD et le nouvel article 7-1 de la loi Informatique et Libertés.** Une disposition visant une limite d'âge pour l'accès à certains services du web a été introduite dans les ultimes jours de discussions du paquet relatif à la protection des données personnelles par les négociateurs du Parlement et du Conseil. Ainsi l'article 8 du RGPD[385], intitulé « *Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information* »**,** conditionne la licéité d'un traitement de données personnelles concernant un enfant dans le cadre d'une offre directe d'un service de la société de l'information à un âge minimum de 16 ans[386]. Un traitement de données concernant un mineur de moins de 16 ans peut s'opérer mais requiert l'autorisation de l'autorité parentale qui vaut consentement au traitement[387]. Cette limite d'âge peut être abaissée par les États membres dans la limite d'un âge qui ne peut être inférieur à 13 ans[388].

En France après de vifs débats un consensus s'est dégagé sur un âge de 15 ans qui marque ainsi la « *majorité numérique* »[389] . Un article 7-1 a été inséré dans la loi Informatique et Libertés par la loi relative à la protection des données personnelles du 20 juin 2018 qui comprend trois alinéas ainsi rédigés : « *En application du 1 de l'article 8 du règlement(UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à partir de l'âge de quinze ans. -Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur.- Le responsable du traitement rédige en termes clairs et simples, aisément compréhensible par le mineur, les informations et communications relatives au traitement qui le concerne.* »

[385] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre-circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JOUE, 4-5-2016, L1119/I-88. Il a été adopté le 14 avril 2016 et est entré en vigueur le 25 mai 2018.

[386] Article 8, 1, alinéa 1, du Règlement (UE) 2016/679 dit « RGPD », *op.cit.*

[387] Ibid.

[388] Article 8, 1, alinéa 2, du Règlement (UE) 2016/679 dit « RGPD », *op.cit.*

[389] V. *Dalloz IP/IT*, numéro 6-juin 2018, le dossier consacré à « La protection de la jeunesse en ligne », et notamment, CHARRIER Benjamin, « Le consentement exprimé par les mineurs en ligne », p.333.

170. ***Plan.*** Or il faut affirmer que ces dispositions trouvent leurs limites s'agissant d'une part de leur objet large que sont les « *services de la société de l'information* » et d'autre part s'agissant de l'application du régime d'un traitement de données à caractère personnel visant le consentement des titulaires de l'autorité parentale **(a).** Il convient en réalité de mettre en œuvre une politique publique de protection des mineurs s'agissant des réseaux sociaux **(b).**

a. L'ineffectivité du recueil de consentement des titulaires de l'autorité parentale pour tout service de la société de l'information

171. **Le champ d'application trop large de la disposition**. Les services de la société de l'information tels que définis à l'article 1(2) de la directive 98/34/CE recouvrent : « *tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération à distance par voie électronique et à la demande individuelle d'un destinataire de services* »[390]. Il faut ainsi différencier ces services de ceux relevant des communications électroniques qui visent la mise en œuvre de communications sur le réseau, à savoir des échanges de contenus de personne à personne. Il s'agit donc des services du web. Ainsi cette disposition vise de manière générale tous les sites du web qui offrent directement un service que ce soit les applications du type réseaux sociaux ou les sites de commerce en ligne[391].

De fait depuis le 25 mai 2018, date d'entrée en vigueur du RGPD, les formulaires de création de comptes de manière générale invitent désormais l'internaute à affirmer qu'il a plus de 16 ans. Que l'on veuille acheter une robe sur le site *Asos* ou s'abonner au journal en ligne *Le Monde,* il faut déclarer avoir l'âge requis en cochant la case dédiée. Or cette généralisation a non seulement peu de sens mais de fait ne peut être effective. La déclaration de l'internaute n'opère aucun contrôle valable de son âge et ne réalise que très imparfaitement une information à l'égard des mineurs. Il faut pour les protéger définir une politique publique qui n'a pas à ressortir de la protection des données personnelles.

172. **L'ineffectivité du consentement requis**. En effet d'autre part il peut être déploré que la protection des mineurs s'agissant des services du web intervienne à travers le prisme de la protection des données personnelles et de l'obligation de consentement de la personne au traitement qui l'innerve.

[390] Directive 98/34/CE du Parlement Européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et règlementations techniques et des règles relatives aux services de la société de l'information (JO L 204 du 21.7.19987, p.37.

[391] V. Directive 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. JOCE L178/1-16.

Il ne doit pas s'agir pour les parents de consentir à un traitement au nom de leur enfant mais d'être contraints par les pouvoirs étatiques confrontés à un enjeu de société. A cet égard le point n° 2 de l'article 8 fait apparaître la difficile mise en œuvre de cette logique de consentement puisqu'il énonce que : « *Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles* ». Il faut être très circonspect sur la mention des moyens technologiques disponibles : en quoi permettent-ils une vérification de l'identité du titulaire de l'autorité parentale ? De la même manière, l'alinéa 2 du nouvel article 7-1 de la loi Informatique et Libertés requiert cette autorisation mais ne précise pas dans quelle mesure elle peut se mettre en œuvre. Faut-il considérer que les parents établissent par des documents d'identité leur lien de filiation avec le mineur de moins de 15 ans, documents d'identité qui de fait ne renseignent aucunement sur l'exercice de l'autorité parentale.

Certes, s'agissant de cette exigence de double consentement la mise en œuvre d'un cookie peut considérer une reconnexion rapprochée dans le temps qui permet de supposer un éventuel double clic de la part de l'enfant et interdire la mise en œuvre du compte. Une mesure bien faible qui sera aisément contournée. La logique ne peut être celle du consentement des parents du mineur ; il faut mettre en œuvre une politique publique qui protège les mineurs en les responsabilisant ainsi que leurs parents.

b. Le contenu d'une politique publique de protection des mineurs s'agissant des réseaux sociaux.

173. **La définition claire des services visés : les réseaux sociaux.** En réalité il s'agit de mettre en œuvre ici une politique publique s'agissant de services web clairement identifiés : les réseaux sociaux du type *Facebook, Snapchat, Instagram, Twitter* ; des services qui permettent d'interagir à travers la création d'un profil avec d'autres individus et ce de manière publique. Cette protection à l'égard des mineurs n'est pas nouvelle. Un site comme *MySpace* dès sa création en 2003 interdit son accès aux mineurs de moins de 13 ans à l'aide d'un formulaire détaillé et de l'implantation d'un cookie le cas échéant. Par ailleurs le site utilise un logiciel d'analyse sémantique qui traque les profils qui pourraient correspondre à des mineurs de moins de 13 ans. Mais comme le souligne très justement Lionel Thoumyre qui a été le directeur « safety and security France » du réseau social, d'autres sites à l'époque

n'appliquaient pas la même politique et il précise qu'ainsi ce public de mineurs pouvait passer à la concurrence[392].

Il est donc nécessaire de fixer un âge limite requis pour accéder à ces services. Il peut être regretté qu'un accord sur l'âge minimal dans le cadre des discussions sur le RGDP n'ait pas été trouvé alors que le minima de 13 ans était approuvé par les associations de défense de l'enfance et qu'il correspondait également à un minimum se dégageant à l'échelle mondiale[393].

174. **Une obligation d'information et de paramétrage à la charge des entreprises du web**. De plus sans requérir un document d'identité à quiconque souhaite s'inscrire sur un site de réseau social, il est nécessaire que la date de naissance de l'internaute soit requise et qu'une information claire sur l'interdiction de l'accès aux enfants se fasse à l'étape de la création du compte par le biais d'un bandeau par exemple. A cet endroit la nouvelle législation dans la pratique montre son ineffectivité alors que cette information ne se réalise que par la requête de la simple mention de l'âge de l'internaute.

Enfin il pourrait être également exigé que de tels services paramètrent par défaut comme non publics tous les profils de mineurs de plus de 13 ans. Dans les faits par exemple Facebook a opéré ce changement. Les CGU du site ont en effet été modifiées sous la pression des pouvoirs publics américains. Evidemment la mesure peut être contournée, un enfant peut renseigner une date de naissance erronée, mais cette pratique illicite ne s'envisage qu'à la marge de la politique publique qui a bien pour but d'informer, de guider et de réguler les pratiques tout à la fois des internautes et des services du web.

§2) La pénalisation dangereuse de la simple consultation d'un site web

175. **L'analogie avec la règlementation de la circulation.** La législation française ne pénalise qu'une seule infraction de consultation qui vise la consultation habituelle de contenus à caractère pédopornographique. Toutefois le débat autour de la pénalisation de la consultation de sites à caractère terroriste resurgit à chaque nouvelle loi dite de sécurité.

[392] Intervention de Lionel Thoumyre lors du Colloque « Les réseaux sociaux, quels enjeux juridiques ? », du 6 mars 2009 organisé par le master 2 « Droit du multimédia et de l'informatique », de l'université de Paris 2.

[393] Voir la règlementation américaine notamment : le « *Children's online Privacy Protection Act of 1998, 15 U.S.C 6501-6505* », qui organise la protection des enfants de moins de 13 ans.

Or il apparaît que la création de ces délits de consultation soulève les mêmes questions que celles posées par la règlementation de la circulation routière. Comme le souligne Jean Morange, cette dernière « *remet en cause des principes fondamentaux du droit, de liberté, d'égalité ou relatif à la présomption d'innocence* » et il rappelle l'utilisation par les juridictions « *d'outils efficaces pour lutter contre l'insécurité routière* » [394].Toutefois il faut considérer ici que l'infraction n'est pas mise en œuvre automatiquement comme peut le faire un radar constatant un excès de vitesse, et comme pourrait le faire penser le caractère technique du réseau. Le simple clic n'est pas sanctionné, ni même la lecture d'un tel contenu alors qu'il faut le consulter à nouveau pour que l'habitude soit constatée.

Toutefois ces délits ne peuvent se multiplier alors que s'agissant de la définition de l'infraction, c'est la consultation en elle-même qui doit être répréhensible et non le contenu mis en ligne **(§1).** Ainsi l'infraction de consultation de sites terroristes introduite dans le Code pénal en 2016 a été déclarée inconstitutionnelle alors qu'elle porte une atteinte manifeste à la liberté d'accéder aux services de communication au public en ligne **(§2).**

A] La difficile pénalisation de l'acte même de consultation

176. ***Plan.*** Si le délit de consultation habituelle de sites à caractère pédopornographique de l'article 227-23 du Code pénal ne pose pas de problème quant à la définition de l'infraction de consultation **(1),** il n'en va pas de même pour le délit de consultation de sites à caractère terroristes. La consultation habituelle de tels sites est d'abord envisagée en 2014 comme un élément cumulatif à la caractérisation d'un acte de terrorisme **(2).**

1) L'article 227-23 du CP visant la consultation habituelle d'images à caractère pédopornographique

177. **La justification de l'article 227-23 du Code pénal visant la consultation habituelle d'images à caractère pédopornographique**. Cette infraction d'habitude a été créée par la loi n°2007-293 du 5 mars 2007 réformant la protection de l'enfance. La lecture des travaux parlementaires fait apparaître l'enjeu de la création d'un tel délit : « *Aujourd'hui, si l'article 227-23 du Code pénal sanctionne bien la détention d'images à caractère pédopornographique, sa rédaction est inopérante pour sanctionner la simple consultation de telles images sur internet : l'emploi du terme « détention » conduit en effet à ne pouvoir incriminer pénalement que les personnes qui ont enregistré des images sur leur disque dur et*

[394] MORANGE Jean, *Manuel des droits de l'homme et des libertés publiques,* Paris P.U.F Droit : 2007 (Manuels, Collection droit fondamental sous la direction de Stéphane Rials), p.149, n°102.

non celles qui se connectent sur ces sites sans conserver de copies des images. C'est la raison pour laquelle le présent article élargit l'incrimination non plus seulement à la détention mais à la consultation habituelle »[395]. En effet, la Cour de cassation dans un arrêt datant de 2005 avait conclu que les traces de la consultation de sites à caractère pédopornographiques dans la mémoire temporaire d'un ordinateur ne suffisaient pas à caractériser l'infraction de détention prévue à l'article 227-23 du Code pénal[396].

Il s'agissait donc d'appréhender une évolution du délit qui vise le caractère répréhensible d'une image ou d'une représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique. Après avoir incriminé la diffusion, la fixation, l'enregistrement et la transmission, se trouve logiquement incriminée la consultation. L'acte déviant se réalise également dans la consultation. De fait cette disposition n'a pas fait l'objet de débat devant les assemblées, ni dans les médias.

Il n'en va pas de même de la consultation d'un site à caractère terroriste.

2) L'article 421-5-6 du CP : la consultation habituelle envisagée comme une condition cumulative à la caractérisation d'un acte de terrorisme

178. **La difficile sanction de la consultation habituelle de sites provoquant et faisant l'apologie du terrorisme.** La sanction de la consultation habituelle de sites provoquant et faisant l'apologie du terrorisme divise alors qu'on s'inquiète de la définition d'une telle infraction et d'une atteinte possible à la liberté d'expression[397]. En effet, la pénalisation intéresse ici la consultation d'un contenu réalisant une infraction de communication. Or le propre d'une telle infraction est qu'elle est susceptible d'appréciation. Par ailleurs, comme tout acte de politique pénale, la création d'une infraction de communication répond d'un contexte qui ici est d'autant plus fortement ressenti qu'il conduit à condamner un propos, sanction qui intéresse la liberté d'expression de tous.

---

[395] Voir le dossier législatif de la loi n°2007-293 disponible sur le site du Sénat. Fr.

[396] Cass. Crim., 28 sept. 2005, 04-85024, publié au bulletin.

[397] Ainsi le journal *Le Monde* s'interroge : « *Où se situe la limite entre organisation terroriste et parti politique ? Les indépendantistes basques de Batasuna, par exemple, étaient considérés jusqu'en 2009 comme faisant partie d'une "organisation terroriste" par l'Union européenne ; Batasuna reste interdite en Espagne, mais pas en France. La consultation de son site depuis la France pourrait-elle être pénalement condamnable ? Surtout, une telle disposition créerait une législation d'exception, s'appliquant à Internet mais pas aux livres, par exemple. En France, la possession, la vente et a fortiori la lecture de Mein Kampf sont légales depuis 1979, mais la proposition énoncée par M. Sarkozy rendrait, en théorie, la lecture de l'autobiographie d'Adolf Hitler illégale en ligne*. », LELOUP D., « La pénalisation des de la consultation de sites « terroristes », une proposition peu réaliste », article mis en ligne sur le site *Lemonde.fr*, le 22 mars 2012.

En 2014 la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme incrimine pénalement à l'article 421-2-5 du CP le fait de « *provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes* »[398], infraction qui jusqu'alors était condamnée sur le fondement du droit de la presse[399]. L'alinéa 2 de l'article prévoit que les peines sont alourdies si de tels faits ont été commis un utilisant un service de communications au public en ligne[400]. Ainsi la mise en ligne est condamnée mais la loi ne sanctionne pas la simple consultation de ces contenus et ne le peut. En effet ici, aucun élément matériel de l'infraction ne se retrouve dans la consultation et ce à la différence d'une consultation régulière d'images ou de représentations à caractère pédophile alors que c'est l'intérêt même de l'individu pour de telles images qui doit être sanctionné.

179. **L'article 421-2-6 du Code pénal.** Cette habitude de consultation de sites terroristes est toutefois intégrée comme une condition cumulative à la caractérisation d'un acte de terrorisme. Le nouvel article 421-2-6 du CP condamne en effet la commission d'un acte terroriste tel que défini dans le Code pénal[401], constitué par la réunion de deux éléments : d'une part *« 1° Le fait de détenir, de rechercher, de se procurer ou de fabriquer des objets ou des substances de nature à créer un danger pour autrui ; »*, et d'autre part l'un des autres faits matériels suivants, dont la liste mentionne le fait de « *c) Consulter habituellement un ou plusieurs services de communication au public en ligne ou détenir des documents provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie*».

En 2016 toutefois va resurgir le débat d'une telle pénalisation dans le cadre de la lutte renforçant la lutte contre le crime organisé, le terrorisme et leur financement.

B] L'inconstitutionnalité du délit de consultation visant les sites provoquant ou faisant l'apologie d'actes de terrorisme

180. ***Plan.*** En 2016 un nouvel article 421-2-5-2 est introduit dans le Code pénal qui réprime la consultation habituelle de sites terroristes **(1).** Cette disposition est abrogée après avoir été déclarée inconstitutionnelle dès lors que portant une atteinte manifeste et disproportionnée à la liberté de communication **(2).**

[398] Article 421-2-5 du Code pénal. L'alinéa 2 alourdit les peines lorsque les faits ont été commis en utilisant un service de communication au public en ligne.

[399] V. le paragraphe 1er « Provocation aux crimes et délits », l'article 24 notamment, de la loi du 29 juillet 1881 sur la liberté de la presse, disponible dans ses versions successives sur legifrance.fr

[400] Ainsi les peines initialement de cinq ans d'emprisonnement et de 75 000€ d'amende, sont portées à sept ans d'emprisonnement et à 100 000€ d'amende.

[401] Articles 421-1 et 421-2 du Code pénal.

1) *L'article 421-2-5-2 du Code pénal crée par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité des garanties de la procédure pénale*

181. **L'article 421-2-5-2 et sa censure par le Conseil constitutionnel.** La loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement[402] et améliorant l'efficacité des garanties de la procédure pénale introduit un nouvel article 421-2-5-2 dans le Code pénal qui énonce que : « *Le fait de consulter habituellement et sans motif légitime un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service.* ». Il est précisé dans un second alinéa que : *« Constitue notamment un motif légitime tel que défini au premier alinéa la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes.* »

On le voit il est tenté de définir[403] davantage la nature du contenu qui appelle à la sanction de sa consultation habituelle en énonçant que le site qui provoque directement à la commission d'actes terroristes ou en fait l'apologie « *comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie* ». La précision pourtant ne convainc pas. Car si un tel site est d'autant plus dangereux dans l'apologie qu'il met en œuvre, la consultation de ce contenu ne réalise pas plus un acte de terrorisme et ne révèle pas la dangerosité des internautes s'y connectant. Au contraire, il apparaît que ce type de sites agressifs dans leur apologie visent des individus démunis et désœuvrés et les endoctrinent. La considération est celle de la protection de ces individus et de la sauvegarde de l'ordre public[404].

[402] La loi n°2016-731 du 3 juin 2016 « renforçant la lutte contre le crime organisé, le terrorisme et leur financement », JORF du 4 juin 2016, texte 1 sur 119, article 18.

[403] V. le rapport n° 335 (2015-2016) de M. Michel MERCIER, fait au nom de la Commission des lois, déposé le 27 janvier 2016, disponible sur le site du Sénat, sénat.fr

[404] Et la logique doit alors être celle d'une mesure de blocage, v. *supra* chapitre 1er intitulé « *Le régime du blocage d'un site, restriction à la liberté de naviguer*».

2) La décision du Conseil constitutionnel du 10 février 2017 censurant cette disposition

182. **La décision du Conseil constitutionnel n°2016-611 QPC du 10 février 2017**. En 2016 le Conseil constitutionnel est saisi d'une QPC visant cette nouvelle infraction et la déclare inconstitutionnelle ce qui conduit à son abrogation[405].

Le raisonnement s'opère en deux temps. D'une part, il reprend la position tenue dans sa décision sur la loi « HADOPI »[406] et affirme que la liberté de communication de l'article 11 de la DDHC implique la liberté d'accéder aux services de communication au public en ligne[407]. D'autre part, selon une logique classique, il énonce que cette liberté de libre-communication doit se concilier avec l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et de la prévention des infractions. Ainsi il faut rechercher si l'atteinte portée à cette liberté de communication est nécessaire, adaptée et proportionnée à ce but visant la sécurité publique[408].

Dès lors il considère d'abord l'ensemble de l'arsenal judiciaire et administratif visant la lutte contre le terrorisme. Des infractions pénales spécifiques ont été instituées visant à réprimer les actes de terrorisme[409] ; le régime des interceptions de correspondances et des données de connexions comme celui des perquisitions s'est spécialisé en ce sens[410] ; enfin le blocage d'un site peut être ordonné à l'initiative de l'autorité administrative ou du juge pénal[411]. Il questionne ensuite la légalité proprement dite de la mesure et souligne que « *Ces dispositions répriment donc d'une peine de deux ans d'emprisonnement le simple fait de consulter à plusieurs reprises un service de communication au public en ligne quelque soit l'intention de l'auteur de la communication* »[412]. En effet quand bien même la « *bonne foi* » est mentionnée comme fait justificatif, cela n'a pas de sens puisque l'infraction ne vise pas et ne peut viser la sanction de l'intention terroriste[413].

---

[405] *Cons. Const.*, Décision n°2016-611 QPC du 10 février 2017.

[406] *Cons. Const*., *déc*. n°2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, cons. 12.

[407] *Ibid.*, cons. 4.

[408] *Ibid.*, cons. 5.

[409] *Ibid.*, cons. 8.

[410] *Ibid.*, cons. 9 à 11.

[411] *Ibid.*, cons. 12.

[412] *Ibid.*, cons. 14.

[413][413] Comme le souligne le professeur Philippe Ségur : « *Pour autant, les faits matériels constitutifs du délit, quand il s'agit de la seule consultation de sites de propagande, ne présentent ni le caractère de proximité ni le caractère d'univocité qui permettent, en droit pénal général, d'établir un lien entre l'intention et l'infraction principale. En particulier, on ne trouve pas trace ici de la condition « d'intention irrévocable » imposée par la Cour de cassation pour reconnaître un commencement d'exécution (Crim. 5 juill. 1951, Bull. crim. N°198),* SEGUR P., « Le terrorisme et les libertés sur l'internet », *AJDA* 2015, p. 160.

Il conclut alors que *« les dispositions contestées font peser une incertitude sur la licéité de consultation de certains services de communication au public en ligne et, en conséquence de l'usage d'internet pour rechercher des informations.* »[414]. Une formulation éclairante que celle adoptée, visant la licéité de manière générale de l'usage du réseau pour rechercher des informations, qui sied parfaitement à l'analogie opérée dans cette étude qui vise la liberté de naviguer sur le web. Une navigation ne peut intrinsèquement réaliser une infraction. En revanche le suivi de celle-ci réalise la surveillance de l'internaute et c'est à cet endroit qu'une nouvelle problématique apparaît.

183. **L'enjeu de la surveillance des sites et des individus qui s'y connectent**. Si de fait, le principe de légalité pénale s'oppose à la mise en œuvre d'une telle infraction de consultation, la logique même de sa détection questionne plus généralement le respect des libertés de l'internaute. En effet pour que soit constatée l'infraction d'habitude, il faut d'une part identifier ces sites terroristes et surveiller les connexions qui y sont opérées. Or là apparaît la limite d'une infraction de consultation car si ces sites sont identifiés la question est alors de savoir pourquoi étant illicites ils ne sont pas bloqués. La logique démocratique est inversée : le site illicite n'est pas bloqué par les pouvoirs publics mais l'individu laissé face à lui-même devant celui-ci est sanctionné pour y accéder souvent.

En réalité, la problématique est celle de considérer dans quelle mesure l'audience de tels sites peut être mise sous surveillance, pour mettre en œuvre des opérations de renseignement s'agissant d'individus potentiellement dangereux. Les requérants[415] dans le cadre de la procédure pour excès de pouvoir visant le décret n°2015-125 du 5 février 2015 venant préciser la procédure de blocage de sites provoquant à des actes de terrorisme ou pédopornographiques prévue par l'article 6-1 de la LCEN soulignent ainsi très justement qu'à l'endroit de la page indiquant que le site a fait l'objet d'une mesure administrative de blocage[416], il faut s'interroger sur les conditions d'enregistrement des adresses IP qui tentent de s'y connecter. Le Conseil d'Etat rejette ce grief indiquant que si le serveur du ministère de l'intérieur sera techniquement destinataire des données de connexion, il ne sera pas mis en place un système de traitement automatisé de ces données[417].

[414] *Cons. Const.*, Décision n°2016-611 QPC du 10 février 2017, cons. 15.

[415] L'association *French Data Network*, l'association *La quadrature du Net*, et la *Fédérationdes fournisseurs d'accès à internet*.

[416] V. l'article 3, alinéa 4 du décret n°2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

[417] CE n°389140, 2ème /7ème SSR, lecture du lundi 15 février 2016.

Cette remarque renvoie au régime de la surveillance de l'internaute naviguant sur le web, qui ne peut être mise en œuvre arbitrairement, mais doit obéir à des règles strictes pour que soit sauvegardées la liberté d'accès et la liberté de naviguer de celui-ci.

Conclusion Chapitre 2ème

184. **L'encadrement de l'activité des moteurs de recherche**. Le rôle d'un moteur de recherche s'agissant de la liberté de naviguer est essentiel puisqu'en organisant la publicité des ressources disponibles sur le web il permet aux internautes de les atteindre.

La problématique est alors de savoir si son activité doit être encadrée alors que le classement opéré agit comme une contrainte sur les internautes. La réponse est non : il est affirmé dans cette étude que la liberté d'entreprendre du moteur de recherche, qui doit répondre de l'efficacité d'un service commercial, ménage un classement objectif régulé à la marge par le droit de la concurrence. Il ne peut être de classement neutre ; les liens sont discriminés selon une logique algorithmique nécessaire. Elle ne porte pas atteinte à la liberté de naviguer de l'internaute dans la limite de l'incitation à la consultation d'un service spécifié.

En revanche il faut être vigilant s'agissant du mécanisme de retrait d'un lien vers un site du web qui prive toute visibilité de ce service et dans une mesure certaine alors, tout accès à celui-ci. Le déréférencement d'un nom de domaine ne peut être le fait que des pouvoirs publics. Le régime envisagé par la loi française est à bon escient le même que celui visant les mesures de blocage de sites ; il répond d'une police administrative spéciale au contenu défini et faisant l'objet d'une procédure de contrôle. En revanche doit être condamnée toute action en ce sens à l'initiative de particuliers que ce soit sur le fondement de l'article 6-I-2 de la LCEN ou de l'article L336-2 du CPI. Un site du web ne peut être déréférencé après simple notification.

185. **L'encadrement de la restriction de l'accès à certains sites et service du web**. Assuré que tous les sites du web sont mis à sa disposition selon un régime transparent, l'internaute peut toutefois se voir interdire l'accès à un site ou service spécifié. Toutefois cette limitation à la liberté de naviguer est soumise à certains principes.

D'une part un règlement européen a été adopté en février 2018 interdisant le blocage géographique injustifié : un internaute ne peut subir une discrimination s'agissant de la mise en œuvre d'un service de commerce électronique en fonction de la nationalité de son point de connexion. Ainsi de la même manière que la réalisation d'un marché commun a permis le développement d'une liberté de circulation des citoyens de l'Union, ce régime vise la réalisation d'un marché unique numérique assurant la liberté de naviguer sur le web européen des citoyens de l'Union.

Par ailleurs, le régime éprouvé de police administrative spéciale visant la protection des mineurs trouve à se développer s'agissant de certaines activités règlementées ayant migré sur le réseau. Ainsi les mineurs ne peuvent accéder à des sites de jeux d'argent en ligne ; de fait de tels services appliquent efficacement la législation en requérant de leurs utilisateurs un document d'identité. Une pratique qui pourrait être élargie au secteur de la vente d'alcool en ligne.

En revanche il faut être réservé sur les dispositions du RGPD qui ont conduit à l'insertion du nouvel article 7-1 de la loi Informatique et Libertés établissant la majorité numérique à 15 ans. D'une part la mention d'une interdiction, d'une manière générale, de l'accès de ces mineurs aux services de la société de l'information ne parait pas pertinente. D'autre part ce régime gagnerait à se dissocier de l'exigence de consentement du régime de la protection des données qui vise ici à vérifier celui du parent ou du titulaire de l'autorité parentale pour permettre l'accès à un enfant de moins de 15 ans.

Or l'accès aux réseaux sociaux ne peut ressortir de la logique d'une activité règlementée qui serait interdite, ou à défaut autorisée si le parent y consentait, ce qui de fait ne peut jamais être s'agissant d'une interdiction mise en œuvre par l'État et visant la protection d'un mineur. L'accès aux services de la société de l'information et notamment des réseaux sociaux doit en réalité faire l'objet d'une politique publique qui a bien pour but d'informer, de guider et de réguler les pratiques tout à la fois des internautes et des services du web.

186. **Le non-sens des délits de consultation.** De plus les individus ne peuvent être contraints dans leur navigation par la pénalisation de la consultation habituelle de certains sites.

La législation française ne pénalise qu'une seule infraction de consultation qui vise celle, habituelle, de contenus à caractère pédopornographique, et seul ce type de contenus peut fonder un tel délit. Le débat s'agissant de la pénalisation de la consultation habituelle d'un site terroriste doit être clos. Quand bien même l'infraction cherche à être définie par la mention d'un contenu spécifié comme des images ou représentations montrant des atteintes volontaires à la vie, la consultation d'un tel site ne réalise jamais une intention de commettre de tels actes. Comme le souligne le Conseil constitutionnel dans sa décision du 10 février 2017, une telle disposition fait peser de manière générale des incertitudes sur la licéité de l'usage d'internet pour rechercher des informations, ce qui ne peut être. La navigation sur le web ne réalise en soi aucune

infraction et l'individu doit être libre de consulter tout contenu mis en ligne, ce qui n'équivaut pas à dire évidemment, que toute mise en ligne est licite.

Ainsi si ces sites ne sont pas bloqués par les pouvoirs publics, la problématique en réalité est de considérer dans quelle mesure l'audience de tels sites peut être mise sous surveillance, dans le cadre d'opérations de renseignement s'agissant d'individus potentiellement dangereux, en vue de prévenir ces actes de terrorisme.

Conclusion TITRE II

187. **La consécration d'une nouvelle liberté publique**. La consécration de la liberté d'accès au réseau conduit nécessairement à celle de la liberté de naviguer sur l'application emblématique de celui-ci, qu'est le web. Toutefois si cette liberté se réalise spontanément, il convient de la sauvegarder en règlementant la possibilité qu'on puisse agir sur la structure du réseau en bloquant certains sites, ou qu'on puisse restreindre l'accès à certains sites, via des politiques discriminatoires à l'égard de certains citoyens.

Ainsi il a été vu que des mesures de blocage interviennent à l'endroit de la structure même du réseau ; elles visent les opérateurs de communications électroniques qui doivent filtrer les URL requis auprès de leurs abonnés et ce de manière pérenne dans le temps, ce qui a un coût. Elles ne peuvent ressortir de la volonté des particuliers. Quand bien même l'action est mise en œuvre par un juge judiciaire, celle-ci n'est pas protectrice de la liberté de naviguer de tous si *ab initio* la mesure ressort de la seule volonté d'un particulier. Ainsi les mesures de blocage ne doivent intervenir qu'à l'initiative des pouvoirs publics selon un régime strict alors que trop largement envisagées elles pourraient porter atteinte à la libre-navigation des internautes.

S'agissant de la règlementation de la consultation des sites et services du web, les internautes doivent être assurés que, en dehors de ces mesures de blocage, tous les sites du web sont mis à leur disposition. La liberté d'entreprendre d'un moteur de recherche doit ainsi être sauvegardée alors qu'elle permet une dynamique de recherche efficace. Le déréférencement d'un nom de domaine ne peut ressortir que du même régime qu'une mesure de blocage et ne peut être laissé à l'initiative d'un particulier. Toutefois l'internaute peut se voir interdire l'accès à un site ou service spécifié, une mesure obéissant à des principes qui fondent sa légalité. Enfin s'il est tout à fait légitime de pénaliser la simple consultation, habituelle, de sites pédopornographiques, ce type de délit ne saurait se multiplier alors qu'aucune autre consultation ne peut être considérée comme illicite en soi.

CONCLUSION PARTIE 1

188. **Le contenu de la liberté d'accès et de la liberté de naviguer sur le web.** Etablissant une analogie avec la sûreté personnelle et la liberté d'aller et venir garanties à l'individu dans le monde physique, la première partie de la thèse a consacré deux libertés : la liberté d'accès au réseau et la liberté de naviguer sur le web.

La liberté d'accès au réseau implique de définir le contenu d'un service public de l'accès ; un objectif mis en œuvre par la loi pour une République numérique adoptée en 2016, même si l'on peut regretter que ce principe de liberté d'accès au réseau n'ait pas été formulé. Cette exigence de service public délimite les contours du principe de neutralité à mettre à la charge des opérateurs de communications électroniques, qui relève d'une conciliation entre les mécanismes d'une économie de marché et la défense de l'intérêt général. Par ailleurs il a été démontré que la coupure d'accès au réseau ne peut être le fait que du juge judiciaire.

La liberté de naviguer sur le web questionne pour sa part le régime permettant le blocage des sites web. Seuls les pouvoirs publics doivent être à même de contraindre la structure du réseau dans le cadre d'une police administrative qui toutefois ne peut être que spéciale. Des restrictions à la liberté de naviguer peuvent par ailleurs intervenir s'agissant de l'accès même de l'internaute à certains services.

189. **La sauvegarde de ces libertés**. Ces deux libertés définies et garanties par un régime de principes adéquats, elles n'ont de sens que si l'individu a accès au réseau anonymement. En effet, l'individu n'est pas libre si l'ensemble de ses actions peuvent être automatiquement reliées à son identité civile et si sa navigation fait l'objet d'un suivi arbitraire.

190.

Deuxième partie : Les principes à mettre en œuvre pour sauvegarder ces libertés

191. **La sauvegarde des libertés d'accès et de naviguer de l'internaute**. La garantie d'un accès au réseau à tout individu et la mise en œuvre d'un régime visant l'encadrement des restrictions à la liberté de naviguer sur le web, une fois celui-ci mis à disposition, n'a de sens que si l'internaute n'est pas arbitrairement surveillé. L'internaute n'est pas libre d'accéder au réseau s'il est identifié pour ce faire ; il n'est pas libre de naviguer entre les points de celui-ci si ses choix de connexion sont connus.

Or la caractéristique du réseau internet est d'être une technologie productrice de traces. La connexion d'un internaute est individualisée grâce à une adresse IP et tous ses choix de navigation sont matérialisés à son insu par les adresses IP associées aux sites web visités. Ces données sont nécessairement produites pour mettre en œuvre la communication sans qu'il y ait besoin d'élaborer un système de surveillance spécifique.

Ainsi au regard de l'émergence de la formule du « Big Data », il faut entendre le mot « big » comme se référant utilement au spectre du *Big Brother* d'Orwell alors qu'une surveillance peut s'opérer à l'insu de l'utilisateur du réseau[418]. Le « dataming » ou « extraction de données » n'est plus ; s'opère aujourd'hui une « dataveillance »[419]. Le « Big data » définit ainsi l'usage de l'intelligence artificielle non pas dans un but d'optimisation de la transmission d'informations mais de surveillance des individus, pour assouvir le fantasme qui en découle, celui de prévoir les comportements.

[418] Il est intéressant de noter que non seulement la surveillance mais également la capacité prédictive permise par l'exploitation des données ne peut naître que de l'ignorance du processus par les individus. Ainsi comme le souligne Vagelis Hristidis, professeur invité en sciences informatiques à l'université de Californie à Riverside : « *un outil censé prévoir les comportements des marchés ne peut fonctionner que si les gens ne savent pas qu'il existe* ». V. : EUNJUNG CHA Ariana, « Le partage des données nous sauvera-t-il ? », article publié initialement dans le *Washington Post* et repris dans le *Courrier international* n°1130 du 28 juin au 4 juillet 2012, p.40

[419] V.: Jason MILLAR, "Core privacy: a problem for predictive data mining" in *Lessons from identity trail, anonymity, privacy and identity in a networked society*, edited by I.KERR, V.STEEEVES, and C.LUCOCK, Oxford University Press, 2009. Oscar H. GANDY, "Data Mining and surveillance in the post 9/11 environment" in *The intensification of surveillance, Crime terrorism and Warfare in the information age*, K.BALL & §F. WEBSTER (*dir.*), PLUTO PRESS 2004. Daniel SOLOVE, *The digital person, technology and privacy in the information age*, New-York University Press, 2004, p.33.

192. **La problématique de la surveillance de l'internaute**. La problématique de la collecte des traces numériques est celle de la surveillance de l'individu. Elle ne relève pas de la protection de sa vie privée et de la liberté de ses choix conscients. Il ne s'agit pas d'investir l'individu d'une action de défense d'un espace d'intimité qui lui correspond mais bien de l'assurer que sa liberté individuelle est garantie. Le parallèle peut être fait avec le monde réel où la sûreté de l'individu, entendue dans le sens large que lui donne le professeur Rivero,[420] interdit toute surveillance policière continue et généralisée [421].

Ainsi sur le réseau il ne s'agit pas seulement d'envisager les conditions de la mise en œuvre d'une surveillance mais de considérer les contours d'un nouvel objet à protéger : les traces laissées par un individu quand il navigue sur le réseau souvent nommées de manière générale comme *« les données de connexion* ». Un terme absent de la législation française jusqu'à la codification récente, en 2012, du Code de la Sécurité intérieure dont l'un des chapitres est intitulé « *Des accès administratifs aux données de connexion* ».

Or il convient d'une part de lever le voile sur cette formulation très peu claire de « *Données de connexions* » dont la généralité peut prêter à confusion. Il est proposé dans cette seconde partie de faire un parallèle avec le monde réel, et d'affirmer que l'identification automatique et le suivi généralisé de tous les faits et gestes d'un individu ne peut être. Ainsi il ne peut être envisagé de considérer un régime visant d'une manière générale des données dites « *de connexion* » ou « *de trafic* », c'est l'individu qu'il faut protéger et il convient de partir dès lors d'un ou plusieurs objectifs fondamentaux pour descendre ensuite dans le détail des données techniques produites et considérer leur encadrement.

---

[420] En ce sens qu'elle permet l'« *exercice paisible* » des libertés de s'informer, de s'exprimer, d'agir sur le réseau. RIVERO Jean MOUTOUH Hugues, *Libertés publiques,* Tome I, 7ème éd. Paris : P.U.F Droit, 2003, p.45 (Thémis droit public).

[421] L'individu ne peut en effet se sentir libre d'une quelconque action s'il est laissé dans le doute quant à une surveillance qui pèserait sur lui. Cette pression qu'exercerait une surveillance arbitraire renvoie à un régime totalitaire ; dès la troisième page du roman d'Orwell *1984* cette caractéristique de la surveillance opérée par un tel régime est soulignée *« Naturellement, il n'y avait pas moyen de savoir si, à un moment donné, on était surveillé* ». V. : ORWELL G., *1984,* Paris : Gallimard, 1950 (*folio, janvier 2008, p.13)*. L'architecture concrète du panoptique développée par Foucault, d'après Bentham, où « *le détenu ne doit jamais savoir s'il est surveillé ; mais il doit être sûr qu'il peut toujours l'être* » montre d'ailleurs que la pression d'une surveillance peut garantir à elle seule la privation de liberté physique de l'homme. Ainsi comme le souligne Foucault : « *De là, l'effet majeur du panoptique ; induire chez le détenu un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir* » et indiquant que ce pouvoir « *est d'autant moins corporel qu'il est plus savamment physique* ». V. : FOUCAULT M., *Surveiller et Punir, naissance de la prison,* Paris : Gallimard (*tel),* 1975, (impression 20 janvier 2007, p. 234). Le philosophe Jacques Derrida l'énonce ainsi: « *la terreur opère si on peut dire, comme d'elle-même, par le simple effet d'un dispositif ».* V. : *Le « concept » du 11 septembre, dialogue à New-York (oct. déc. 2001) avec Giovanna Borradori, Jacques Derrida, Jürgen Habermas*, Paris : Galilée, 2004, p. 163.

193. **Le respect de la liberté individuelle de l'internaute**. Jacques Georgel, professeur de droit public, critiquant à la fin des années quatre-vingt dix l'essor de la surveillance de l'espace public mise en œuvre par des dispositifs de caméras-vidéos, analyse justement que celle-ci, durable et inaperçue, conduit à considérer que « *Marcher la tête en l'air n'est pas recommandé* ». Or ce constat ne peut être dans un État de droit : la sûreté contre tout arbitraire qui fonde le principe de liberté d'un État démocratique ne se conçoit que, parce qu'en marchant à visage découvert[422], le citoyen est identifiable et peut donc répondre de ses actes. Il doit en aller de même sur le réseau.

Toutefois alors que la réalité des données produites n'est pas saisie, la liberté individuelle de l'internaute est annihilée aujourd'hui sur celui-ci car le raisonnement s'agissant de la liberté de l'internaute se réduit à deux propositions extrêmes et antagonistes : soit l'internaute considère qu'il est libre car il n'a rien à cacher[423], soit il considère qu'il est libre car il avance le visage masqué.

194. ***Plan.*** Or il faut affirmer que la liberté d'accès n'a de sens que si un régime organise le respect de l'anonymat de l'internaute connecté au réseau **(Titre I)**. Par ailleurs la liberté de naviguer ne se conçoit que si est encadrée la surveillance de l'internaute naviguant sur le web **(Titre II)**.

Titre I. Le respect de l'anonymat connecté au réseau

Titre II. Les limites à la surveillance de l'individu naviguant sur le web

[422] V. loi 2010-1192 du 11 octobre 2010 sur la dissimulation du visage dans l'espace public.

[423] L'expression est empruntée au professeur de droit américain Daniel J. Solove. V. son ouvrage : SOLOVE D.J., *Nothing to Hide, The False Trade between Privacy and Security,* Yale University Press, 2011.

TITRE I. LE RESPECT DE L'ANONYMAT DE L'INTERNAUTE CONNECTE AU RESEAU

195. **Le respect de l'anonymat de l'internaute**. L'anonymat est défini comme *« l'état de quelqu'un, de quelque chose qui est anonyme* », c'est-à-dire « *dont on ignore le nom* ». L'anonymat de l'internaute doit ainsi s'entendre : l'internaute connecté au réseau et agissant sur celui-ci n'a pas besoin pour ce faire de décliner son identité. Ce qui ne veut pas dire qu'il ne peut pas être retrouvé. L'internaute doit être anonyme sur le réseau de la même manière qu'il l'est dans le monde réel : lorsqu'il se connecte et navigue sur le réseau on ignore son identité mais il peut être identifié a posteriori par un procédé d'investigation.

La difficulté sur le réseau est qu'alors qu'aucune interaction physique ne peut se mettre en œuvre avec l'internaute, cette nuance achoppe sur la technicité des données et l'automatisme des procédés que le réseau met en œuvre. Ainsi soit la technicité de l'adresse IP faire dire qu'elle ne permet jamais d'identifier l'individu, soit l'automatisme de la production de cette donnée fait dire que l'individu peut nécessairement être retrouvé.

Ainsi pour certains, la technique de l'adressage du réseau empêche tout anonymat ; les partisans d'un internet dit « libre » prônent alors l'usage d'un logiciel comme « TOR » qui masque l'adresse IP à l'origine de la connexion et qui empêche tout lien entre un internaute et ses faits et gestes sur le réseau. Pour d'autres la seule visualisation d'une adresse IP sur le réseau ne permet pas l'identification de l'individu et il faut remédier à cet anonymat souvent qualifié de « général » ou de « total », en ce sens qu'il ne peut jamais être levé.

196. **La problématique du champ d'application de la protection des données personnelles.** La difficulté est que ce raisonnement n'est pas éclairci par la tentative d'application de la protection des données personnelles à l'adresse IP. En effet la définition de la donnée à caractère personnel et celle du traitement de données, telles que largement interprétées et dissociées aujourd'hui dans leur approche, sont ici inadéquates. D'une part l'adresse IP est l'identifiant[424] d'une connexion mais pas d'un individu alors qu'un procédé d'investigation est nécessaire pour identifier à partir de cette donnée un internaute. D'autre

[424] Un identifiant est défini comme : « un code alphanumérique permettant d'identifier de manière unique une information afin de pouvoir s'y référer de manière univoque ». Entrée « identifiant », *Le Petit Robert*, 2013. Ainsi un identifiant ne s'inscrit pas dans un processus d'inférence pour identifier, il identifie.

part l'adresse IP étant par essence numérique, la notion de collecte d'une telle adresse par quiconque la visualise sur le réseau ne peut avoir de sens.

La problématique du champ d'application de la loi Informatique et Libertés est qu'elle ne peut se départir du contexte qui l'a vu naître et qui tendait à encadrer les fichiers de données qui permettaient une identification automatique de l'individu. Ainsi soit la personne était identifiée directement et des informations étaient réunies sous son nom, soit l'identité de la personne n'apparaissait pas dans le fichier mais était substituée par un numéro identifiant qui lui était attribué. Ce que l'on cherchait à encadrer était l'identification automatique, directe ou indirecte, de l'individu. Or l'interprétation large du champ d'application de la loi qui a cours aujourd'hui et qui considère que toute donnée est personnelle dès lors qu'elle est relative à un individu identifié ou identifiable et qu'il y a traitement dès lors qu'il y a collecte, dilue cet objectif.

197. **L'adresse IP : le visage découvert de l'internaute**. Si l'on s'extrait du débat sur la nature personnelle de l'adresse IP et la notion de traitement eu égard au fonctionnement du réseau, la problématique apparaît : il faut considérer dans quelle mesure l'adressage du réseau permet une investigation efficace s'agissant d'identifier l'internaute à partir de son adresse IP et envisager alors comment un tel mécanisme peut être encadré.

Filant l'analogie adoptée dans cette étude qui compare le réseau avec le monde physique, il sera montré que l'adresse IP donnée à la connexion de l'internaute peut être comparée à son visage. Lorsqu'un individu entre dans un commerce, la simple visualisation de son visage ne peut conduire le commerçant à son identification et il faut s'en garder[425]. Cependant la description des caractéristiques de celui-ci ou la délivrance de l'enregistrement pris par une caméra de vidéosurveillance aux personnes et autorités compétentes qui détiennent les éléments de son identité peut permettre celle-ci.

Ainsi dans le monde physique, tous les faits et gestes d'un individu peuvent être reliés à son identité. La liberté individuelle de l'internaute est respectée alors que pour ce faire une investigation est nécessaire et qu'elle répond d'un régime légal qui ne peut être mis en œuvre que par les pouvoirs publics. Il doit en aller de même sur le réseau.

198. ***Plan*.** Ainsi dans un premier chapitre, il sera tenté de mettre fin au débat visant la qualification de l'adresse IP en tant que donnée à caractère en démontrant que l'adresse IP est un moyen d'établir l'identité de l'internaute **(Chapitre 1er).** Cette démonstration faite, il

[425] Le visage d'un individu n'est ainsi pas une donnée personnelle. Il ne va le devenir que dans le cadre de la mise en œuvre d'un procédé biométrique qui associe à ses caractéristiques de manière automatique une identité.

pourra être considéré, dans un second chapitre, dans quelle mesure doit être encadré l'adressage du réseau pour permettre cette investigation (**Chapitre 2ème).**

Chapitre 1er. L'adresse IP, un moyen d'établir l'identité de l'internaute connecté

Chapitre 2ème. L'encadrement de l'identification de l'internaute à partir de son adresse IP

Chapitre 1er. L'adresse IP, un moyen d'établir l'identité de l'internaute

199. **La limite du champ d'application élargi de la protection des données personnelles s'agissant de l'adresse IP**. Il faut affirmer que l'adresse IP peut être reliée à un individu identifié, l'abonné et à un individu identifiable, l'internaute connecté au réseau.

En effet un opérateur de communications électroniques attribue cette adresse à la connexion de l'un de ses abonnés. Il est à même de mettre en œuvre un fichier qui permet d'associer automatiquement une adresse IP aux coordonnées d'une personne morale, comme une collectivité ou une entreprise ou à ceux d'une personne physique, comme un particulier. Dès lors en considération des coordonnées de cet abonné, et surtout de la localisation physique du point d'accès auquel a été attribuée l'adresse IP, une investigation efficace peut être mise en œuvre pour découvrir l'identité de l'internaute à l'origine de la connexion

Toutefois il faut se garder d'affirmer que l'adresse IP est l'identifiant d'un individu. En effet quand bien même cette adresse est par essence une donnée numérique, elle ne permet jamais une identification automatique de l'internaute. Une investigation est toujours nécessaire pour ce faire. Or cette nuance entre numérisation et automatisme de l'identification ne peut être faite par la systématisation qu'opère aujourd'hui la loi Informatiques et Libertés qui envisage la nature personnelle d'une donnée en soi. Il faut condamner ce raisonnement qui dissocie le caractère personnel d'une donnée des contingences de son traitement.

200. **Aucune donnée n'est personnelle en soi.** Ainsi il faut rappeler qu'il a été très justement soutenu que la seule mention du nom patronymique sur un site Web ne peut conduire à identifier un individu et il a été conclu qu'il n'était pas une donnée personnelle[426]. Toutefois il est évident qu'on ne peut affirmer que le nom patronymique ne permet pas

[426]TGI Paris, 22 septembre 2008, réf., M. Kalid O. c/sté Notrefamille.com, cf RLDI 10-2008 n°42 Actualités, obs. L. Costes. De fait une fois ce contentieux de la nature personnelle ou non du nom mis en ligne évacué, la réelle problématique est apparue alors que si la loi impose un libre-accès des citoyens aux documents publics sous toutes leurs formes, il faut s'interroger sur la commercialisation d'une base de données d'archives dont le coût de la numérisation a été pris en charge par une administration, v. CE 10ème-9ème ch. réunies, décision du 8 février 2017, notrefamille.com/département de la Vienne.

l'identification d'un individu[427]. Le raisonnement est le même pour l'adresse IP : elle n'est pas l'identifiant d'un individu et ne peut conduire à une identification automatique d'un individu, mais disant cela, il serait erroné de conclure qu'elle ne permet pas d'identifier l'internaute derrière son ordinateur.

Il faut ainsi revenir aux raisonnements de la fin des années 2000 qui soutenaient que l'adresse IP était une donnée personnelle mais qu'elle ne l'était pas toujours, le contexte implicite de la donnée devant être pris en compte. Peter Hustinx, par exemple, contrôleur européen à la protection des données affirme en 2009 : « […] *Les adresses IP devraient être considérées comme des données à caractère personnel dans de nombreux cas mais pas nécessairement dans tous les cas. Le contexte dans lequel s'inscrit un cas donné est important, en particulier si « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre soit par le raisonnable du traitement » doit être évalué. Toutefois en pratique l'allégation selon laquelle les adresses IP ne devraient pas être considérées comme des données à caractère personnel dans tel ou tel cas semble nécessiter davantage d'explications que celle selon laquelle elles constituent bien des données à caractère personnel* »[428].

L'adresse IP ne peut être considérée comme une donnée personnelle en dehors de l'appréciation des conditions d'accès au fichier l'associant au point d'accès physique au réseau utilisé. La deuxième partie de l'affirmation du contrôleur européen à la protection des données souligne maladroitement l'enjeu d'une telle adresse : elle peut permettre le contrôle de l'identité de l'internaute et de ce fait doit faire l'objet d'un régime protecteur.

201. **L'adresse IP, une adresse**. L'adresse IP est une adresse qui localise dans le monde physique un point de connexion au réseau et qui permet dès lors de retrouver l'internaute qui s'est connecté à partir de ce point.

Dans une conférence donnée à l'École polytechnique en 2005, le philosophe Michel Serres rappelle ainsi la racine du mot adresse, révélée davantage par la langue anglaise et les deux « d » qu'elle utilise : l' « ad-dress », vient du latin « Ad Rex ». L'adresse est là, dit M. Serres, « *pour que le roi, enfin celui qui a le pouvoir puisse m'envoyer la police si par hasard j'ai commis une infraction, un délit ou un crime ou*

[427] V. l'entrée « identité civile », in CORNU G., Association Henri Capitant, Vocabulaire juridique, 11ème éd., Paris : PUF (Quadrige), « Ensemble des éléments qui, aux termes de la loi, concourent à l'identification d'une personne physique (dans la société, au regard de l'état civil) : nom, prénom, date de naissance, filiation, etc. ».

[428] HUSTINX P. « Protection des données à caractère personnel en ligne : la question des adresses IP », *Légicom*, n°42-2009-1, p.125. V. également : Avis 4/2007 sur le concept de donnée à caractère personnel, adopté le 20 juin 2007, 01248/07/FR WP 136.

celui qui détient le pouvoir peut me retrouver si je n'ai pas payé l'impôt […] C'est donc un espace métrique en même temps qu'un espace politique, un espace de pouvoir »[429]. L'espace métrique ne se retrouve pas dans un réseau de communication tel que l'internet. Pourtant la dénomination même d' « adresse » qui est donnée à la suite de nombre que forme l'IP est comprise de tous.

Lorsqu'on s'enquiert auprès de n'importe quel quidam de ce qu'est une adresse IP, il répond qu'elle permet de retrouver un internaute à l'origine d'une connexion, et de citer pour exemple les condamnations de contrefacteurs qui se livraient à de la mise en ligne de contenus illégaux ou la possibilité qu'a la HADOPI de retrouver tout internaute grâce à ce numéro. La logique de la trace permise par l'IP et *a contrario* celles des difficultés pour retrouver un internaute si celle-ci est masquée ou a été usurpée est connue par tous désormais.

202. **La problématique du champ d'application de la loi Informatique et Libertés.** La problématique s'agissant de l'adresse IP a été celle de savoir si une telle donnée entrait dans le champ d'application de loi Informatique et Libertés. Dans les premiers temps du réseau, en application de la logique de l'information « *indirectement nominative* », un consensus s'établit. Le fournisseur d'accès par le truchement du fichier qu'il met en œuvre peut associer ce numéro à un abonné.

Cependant l'évolution du champ d'application de la protection des données personnelles va conduire à des hésitations s'agissant de sa qualification. Selon la nouvelle définition de la donnée à caractère personnel, l'adresse IP qui peut être reliée à un individu identifié, l'abonné, est une donnée personnelle. Toutefois cette approche visant le « *potentiel d'identification* » d'une donnée a du mal à être circonscrite ; et le cas de l'adresse IP est topique de la limite de ce nouveau concept. En effet ce potentiel d'identification doit-il être considéré relativement, c'est-à-dire eu égard aux conditions d'un traitement spécifique de l'information ou objectivement, à savoir dans l'absolu ? Dans cette seconde hypothèse, toute adresse IP visible sur le réseau est une donnée personnelle. Dès lors qu'elle est collectée et amenée à être traitée automatiquement ou à intégrer un fichier, les prescriptions de la loi Informatique et Libertés s'appliquent quand bien même ces opérations ne permettent pas une identification automatique de

[429] V. : « Les nouvelles technologies, que nous apportent-elles ? », conférence de Michel Serres, enregistrée à l'École Polytechnique le 1er décembre 2005, faisant partie du cycle *Culture Web*, coordonné par Serge Abiteboul, dans le cadre des Thématiques INRIA. Disponible au format mp3 sur le site : interstices.info, rubrique « débattre ».

l'individu puisque le responsable du traitement n'a pas accès aux données détenues par le FAI.

Le contentieux de la lutte contre le téléchargement illégal qui se développe sur les plates-formes dites de P2P à la fin des années 2000 va soulever cette problématique et diviser les juges. Aujourd'hui il est constant d'affirmer que l'adresse IP est une donnée personnelle, une qualification qui laisse encore toutefois des questions en suspens, et qui selon cette étude doit être reconsidérée.

203. ***Plan.*** Ainsi dans un premier temps il faudra détailler le fonctionnement de l'adressage du réseau **(Section I)** ce qui permettra dans un second temps de comprendre et de s'interroger sur la reconnaissance jurisprudentielle du caractère personnel de l'adresse IP **(Section II)**.

Section I. Le fonctionnement de l'adressage du réseau

204. **La fonction de l'adresse IP**. La définition de l'adresse IP qui est une suite de nombres tient en réalité dans l'exposé de sa fonction. L'adresse IP indique de manière unique un terminal qui met en œuvre une connexion au réseau mondial de communication qu'est internet. Autrement dit de la même manière qu'un numéro de téléphone permet à un destinataire d'être joint, une adresse IP permet la mise en œuvre d'une connexion au réseau.

En effet, un système de communication que l'on oppose à un mode de diffusion implique un échange : il y a interactivité entre deux machines qui peuvent tout à la fois être émettrice et réceptrice du signal. Or pour que des informations puissent transiter entre ces deux machines, il faut leur attribuer une adresse. Sur le réseau internet on parle d'adresses IP[430]. Le réseau des réseaux n'a ainsi pu naître qu'une fois trouvé un nouveau protocole permettant d'attribuer à n'importe quel point d'accès au réseau une adresse unique permettant la connexion de tous les réseaux existants qui avaient leur propre protocole de communication. Cela devient possible avec le protocole TCP/IP créé par les ingénieurs américains Robert Kahn et Vint Cerf en 1973. L'adresse IP est une suite de quatre nombres compris entre 0 et 255, séparés par des points tels que : 172.16.254.1[431].

[430] Ainsi « chaque paquet de données transmis par le protocole internet (paquet IP) est étiqueté avec deux adresses IP pour identifier l'expéditeur et le destinataire. Le réseau utilise l'adresse de destination pour transmettre la donnée. Le destinataire sait à qui répondre grâce à l'adresse IP de l'expéditeur. », Glossaire multimédia, définition de l'adresse IP www.futura-sciences.net et www.wikipédia.fr

[431] Cette adresse IP est une adresse IP de version 4 dont la forme permet donc 255puissance4 adresses différentes. Un peu plus de 4 milliards de machines peuvent ainsi se connecter en même temps au réseau alors que ces adresses peuvent être réparties dynamiquement entre tous les points d'accès ; c'est-à-dire que considérant que tous les points d'accès n'opèrent pas une connexion en même temps, une même adresse peut être attribuée à deux points d'accès au réseau différents à des moments différents. Malgré ce mécanisme de répartition dynamique, l'adressage du réseau arrive aujourd'hui à saturation alors que le

Il faut ainsi souligner qu'il est impropre d'affirmer que l'adresse IP est l'adresse d'une machine tout comme le numéro de téléphone n'est pas l'identifiant de l'appareil téléphonique mais celui d'une ligne téléphonique qui fait l'objet d'un abonnement. De la même manière l'adresse IP n'est pas l'adresse d'une machine qui serait définie par ses caractéristiques propres et renverrait à son propriétaire.

205. **L'adresse d'un point d'accès au réseau et non de l'ordinateur utilisé pour se connecter**. Une adresse IP est attribuée à un point d'accès que celui-ci consiste en une prise filaire ou un terminal émettant un signal permettant un accès en wifi. Ainsi elle est attribuée à la boucle locale qui opère le raccordement d'un domicile par exemple, avec le réseau filaire mondial. Elle renvoie ainsi à un terminal qui n'est pas l'ordinateur personnel d'un individu mais la « Box » sur laquelle un individu peut brancher son ordinateur via un port « ethernet » et qui émet également un signal à partir duquel il peut se connecter en wifi via un code d'accès.

En conséquence il faudra être réservé sur les définitions qui énoncent que l'adresse IP est le « *numéro d'identification d'un ordinateur en raison de son accès à l'internet* »[432] ou encore que celles-ci sont « *les adresses affectées aux ordinateurs qui dialoguent sur le réseau* »[433]. Certes la notion de connexion est précisée mais la mention d'un ordinateur est impropre et peut entraîner une confusion avec l'adresse MAC qui est la seule adresse propre à un ordinateur. L'on préfèrera les définitions qui affirment que l'adresse IP est « *l'identifiant unique à un instant « t » permettant de distinguer un terminal connecté au réseau d'un autre terminal connecté au réseau* »[434] ou encore celles qui énoncent que l'adresse IP renseigne sur « *l'emplacement sur le réseau* »[435]

---

réseau s'est développé. Il a alors été mis en œuvre une version 6 de l'adresse IP (IPV6) qui permet de multiplier par 4 le nombre d'adresses existantes. V. l'article consacré à l'« IPV6 » sur le site wikipédia.fr

[432] En ce sens il ne faut pas la confondre avec l'adresse MAC. . Cette dernière est physiquement implémentée dans la carte réseau de toute machine par le constructeur.

[432] V. CASTETS-RENARD C., *Droit de l'internet*, Paris : Montchrestien, Lextenso éditions, 2010 (Cours, *coll.*, B. Beigner (*dir.*)), p.111.Céline Castets-Renard précise toutefois par la suite ce rapport au fournisseur d'accès dans sa définition de l'adresse IP : « *L'adresse IP (Internet Protocol) constitue un numéro d'identification d'un ordinateur, en raison de son accès à l'internet. Ce numéro est attribué par le fournisseur d'accès à l'internet au moment de la conclusion du contrat d'accès* » ; « *La question s'est posée de savoir si l'adresse IP d'un ordinateur constitue une donnée personnelle. Si cette adresse est un numéro d'identification de l'ordinateur, et non de la personne, il est possible au fournisseur d'accès de rattacher ce numéro à la personne, puisque le fournisseur attribue lui-même ce numéro à son client au moment de la conclusion du contrat* ».

[433] V. HOLLANDE A. et X. LINANT DE BELLEFONDS, Pratique du droit de l'informatique et de l'internet, Edition Delmas, 6ème éd., Paris, 2008, p.287. Ils précisent que « *Pour des raisons techniques, il est impossible que deux ordinateurs possèdent la même adresse* ». Une affirmation qui est imprécise. Elle pourrait être corrigée ainsi : pour des raisons techniques, il est impossible d'attribuer à deux connexions au réseau une même adresse.

[434] SIMON Ch., « Les adresses IP sont des données personnelles selon le Conseil constitutionnel », *RLDI*, juillet 2009, n°51, 1701.

[435] QUEMENER M., FERRY J., *Cybercriminalité, défi mondial et réponses*, Paris : Economica, 1997, glossaire p.26.

d'une connexion ou permet « *d'identifier l'accès à partir duquel un ordinateur se connecte à internet* »[436].

La mise en œuvre d'une connexion sur le réseau via une suite de nombre ne doit pas masquer la réalité physique de cet accès au réseau. Les paquets IP doivent être transportés jusqu'à un point de la structure qui opère la transmission des informations.

206. ***Plan.*** L'adresse IP renvoie à une fonction : celle de la mise en œuvre d'une communication sur le réseau. Elle renseigne dès lors sur la localisation physique d'un point d'accès au réseau.

Ainsi dans un premier temps il sera vu comment une adresse IP est publiquement reliée à un opérateur de communications électroniques **(A)**. Puis dans un second temps dans quelle mesure celui-ci est à même de localiser le point d'accès auquel il a attribué cette adresse **(B)**.

§1) Le mécanisme public d'attribution d'une collection d'adresses IP aux opérateurs de communications électroniques nationaux

207. **L'internet, un réseau de réseaux**. L'internet est un réseau de réseaux. C'est la signification de ce terme d'origine américaine qui dérive de ceux d'« *internetting* » ou d' « *inter-networks* ». L'idée qui préside à sa naissance est la création d'une structure décentralisée ; les informations ne sont pas transmises, de manière hiérarchisée et donc de manière unique d'un sommet vers une base, elles s'échangent de tous les points de la structure. Toutefois la transmission des informations sur le réseau ne se réalise pas de manière aléatoire, elles doivent suivre un chemin qui obéit à une logique.

En effet la nature même de l'adresse IP qui est un nombre élevé à une puissance permet une fragmentation en plages d'adresses, qui en fonde la répartition. Celle-ci suit un découpage complexe pour faciliter la transmission des informations. Technique et mathématique, cet adressage fait l'objet d'un enseignement spécifique destiné aux ingénieurs et aux informaticiens[437] ; notre étude n'est pas destinée à appréhender ces connaissances. En revanche il est aisé de comprendre que pour que le protocole TCP/IP fonctionne, la répartition des adresses ne peut se faire qu'à l'échelle mondiale selon des règles intangibles qui doivent obéir à un système de publicité.

[436] CARON Ch., « Qualification de l'adresse « IP » : état des lieux jurisprudentiels », *Comm. Com. Electr.*2007 n°12, comm. 144.

[437] V. par exemple, les intitulés de cours dispensés par Patrick MAIGRON, ingénieur d'études et enseignant à l'Institut Télécom/ Télécom Sud Paris (Evry, France), disponibles sur la page personnelle de l'enseignant www-public.it-sudparis.eu/~maigron/, rubrique « enseignements».

208. ***Plan.*** Cette répartition est actuellement dévolue à l'ICANN **(1)** Elle organise l'attribution des adresses entre les différents opérateurs nationaux de communications électroniques **(2).**

A] La répartition opérée par l'ICANN.

209. **La répartition opérée par l'ICANN.** L'ICANN pour « *Internet Corporation for Assigned Names and Number* » est une organisation internationale sans but lucratif créée aux Etats-Unis en 1998. Un débat existe sur l'évolution du statut de l'ICANN[438]. Le propos ici n'est pas d'étudier ces enjeux de la « gouvernance de l'Internet » mais de souligner l'existence de ceux-ci qui démontre que l'adressage d'un espace, quand bien même dématérialisé, est par essence une tâche politique car normative et fondatrice de pouvoirs. L'ICANN a comme son nom l'indique deux fonctions principales : elle assigne des noms et des nombres.

Ces deux fonctions renvoient aux deux points de la communication. En effet, le principe du réseau internet est de permettre à tout individu de se connecter à n'importe quelle machine dans le monde pour y consulter les informations qu'elle stocke. Ainsi il faut différencier l'adressage des machines qui sont connectées au réseau pour mettre à disposition du contenu de l'adressage des machines qui se connectent au réseau pour communiquer. En effet, l'attribution d'une adresse IP à une machine stockant du contenu est pérenne dans le temps et fait l'objet d'une transcription en nom de domaine[439] qui renvoie à la personne qui a réservé celui-ci[440]. En revanche la répartition des plages d'adresses IP affectées à la mise en œuvre des connexions vers ces serveurs est géographique. Ainsi une adresse IP visible sur le réseau porte deux indications mises

[438] V. sur ce point : HUET J., DREYER E., *Droit de la communication numérique,* Paris : L.G.D.J., 2011 (Manuel), point 5 « L'ICANN » et point 9 « L'universalité du net ». BARRE Nicolas, « Contrôler Internet ? », éditorial du journal *Les Echos* du lundi 23 juin 2008.

[439] Le nom de domaine est une adresse en langage courant qui est donc plus facile à retenir pour l'individu que l'adresse numérique. En effet, si un internaute n'a pas besoin de connaître l'adresse qui est allouée à son ordinateur ou à son téléphone lorsqu'il se connecte au réseau, il doit en revanche connaître l'adresse du site qu'il souhaite consulter. Entrer la suite de nombres de l'IP du serveur du site Web s'avèrerait alors une opération fastidieuse. Dès lors un système a été mis en œuvre qui permet à chaque site d'être désigné selon un autre protocole du type : www. nomdusite.extension (L'extension, permet une visualisation claire d'un espace géographique, celui dans lequel le nom de domaine a été enregistré). V. l'avis du G29 34/2000 du 21 nov. 2000 « Le respect de la vie privée sur internet », p.9

[440] C'est l'ICANN qui décide de l'attribution des noms de domaine de premier niveau qui correspondent aux extensions nationales et génériques. L'attribution d'un nom de domaine est ensuite le fait d'autres organismes dit « *registrar* » ou « bureau d'enregistrement » ; ces bureaux nationaux sont en liens avec les clients finaux, qui peuvent être des particuliers, qui souhaitent acquérir un nom de domaine en vue de la mise en ligne d'un site Web. L'ICANN gère d'autre part la correspondance entre les adresses IP localisant les sites Web sur le réseau et le nom de domaine. qui leur a été attribué selon un système de résolution de nom ou système « DNS » en anglais, qui fonctionne comme un annuaire inversé. En effet le réseau fonctionnant selon le protocole TCP/IP, il est nécessaire qu'une table des correspondances soit mise en œuvre à l'échelle mondiale. V. « La racine du DNS : bien commun ou fragmentation » intervention de Patrick MAIGRON , ingénieur à l'institut Télécom/TélécomSudParis, lors du colloque du CEJEM-Université Panthéon-Assas, « Les philosophie de l'Internet : conciliation possible avec le droit, » du 9 juin 2011.

à la disposition de tous : celle d'une zone géographique de connexion et celle d'un opérateur national**.**

210. **L'attribution d'une plage d'adresses IP à un opérateur national**. L'ICANN va en effet répartir les différentes plages d'adresses IP affectées aux différents points d'accès au réseau. Cette répartition est géographique.

Les adresses sont d'abord allouées aux différents registres régionaux d'adresses internet : AfriNIC (Afrique), APNIC (Asie - Pacifique), ARIN (Amérique du Nord), LACNIC (Amérique Latine et Caraïbes) et RIPE NCC (Europe)[441]. Cette répartition suit la division opérée par le premier nombre de l'adresse IP ; un tableau de concordance s'établit alors entre le 1er nombre de l'adresse IP et la zone géographique concernée. Ce tableau est public et est facilement accessible en ligne[442]. Ainsi 32 plages d'adresses IP ont été attribuées au registre européen : 002, 005, 031, 037, 046, 062, 077 à 095, 109, 176, 178, 185, 193 à 195, 212, 213. Par exemple, une adresse IP commençant par 213 renverra nécessairement à un serveur connecté en Europe. Ainsi une adresse IP est nécessairement liée à une zone géographique.

Puis les registres régionaux d'adresses internet (RIR de l'anglais *Regional Internet Registry*) distribuent à leur tour les adresses qui leur ont été attribuées, à des registres locaux (LIR de l'anglais *Local Internet Registry*), qui les attribuent à leur tour aux opérateurs de communications électroniques. Cette répartition est publique. Ainsi en utilisant un outil de type whois[443], n'importe qui est en mesure de connaître l'opérateur national de communications électroniques à qui a été attribuée cette adresse.

B] La population des opérateurs de communications électroniques nationaux

211. **La problématique de la définition légale de l'opérateur de communications électroniques.** La définition légale d'un « *opérateur de communications électroniques* » entend par ce terme « *toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques* » s'applique ici[444]. Cette définition est aujourd'hui questionnée alors que sur le réseau peuvent être dissociées les fonctions de l'opérateur qui met en œuvre

[441] Voir le site internet de Patrick MAIGRON, enseignant à l'INT sud Paris : « Le tour du net en questions », http://www-public.it-sudparis.eu/~maigron/Internet/, rubrique « Adresses IP », qui est d'une grande clarté pour tous, informaticiens ou non, en ce qui concerne l'adressage du réseau.

[442] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

[443] Whois est la « (*contraction de l'*anglais *who is?, signifiant « qui est ? ») est un service de recherche fourni par les registres* Internet*, par exemple les* Registres Internet régionaux *(*RIR*) ou bien les* registres de noms de domaine *permettant d'obtenir des informations sur une* adresse IP *ou un* nom de domaine. », V. l'article consacré à « Whois », fr.wikipédia.org

[444] V. art L32, 15° CPCE.

la structure ou permet la connexion, de celui qui achemine une communication, entendue comme la mise en relation de deux individus[445]. Toutefois cette problématique n'intervient pas ici. Les adresses IP du réseau mondial sont attribuées à l'opérateur de la communication c'est-à-dire à toute entité qui met en œuvre physiquement un accès au réseau ou propose un service d'accès à la boucle du réseau mondial qu'il a mise en œuvre ou à laquelle il a accès.

Ainsi comme le souligne la définition du CPCE, l'opérateur exploite un réseau de communications électroniques ou fournit un service de communications électroniques. C'est-à-dire que soit il a mis en œuvre les câbles, satellites ou antennes qui réalisent le réseau ou alors à tout le moins il a accès à cette infrastructure et propose ses services pour organiser la transmission des données sur celle-ci.

Par ailleurs le CPCE précise que le réseau est « *ouvert au public* » et que le service de communications électroniques est fourni « *au public* ». Un « *réseau ouvert au public* » est défini comme « *tout réseau de communications électroniques établi ou utilisé pour la fourniture au public de services de communications électroniques ou de services de communication au public par voie électronique* »[446] *;* une définition qui en reprenant l'adjectif public éclaire peu sur le sens de celui-ci. La nature du réseau apparaît si on l'oppose au réseau indépendant[447] et au réseau interne[448]. Le réseau ouvert au public met en œuvre des services dont l'usage est ouvert à tous ; l'infrastructure qui le réalise appartient au domaine public.

212. **La population des opérateurs nationaux de communications électroniques.** Ces opérateurs sont identifiés alors qu'ils doivent faire l'objet en France d'une déclaration auprès de l'ARCEP selon l'article L33-1 du CPCE. En effet alors que le secteur des communications électroniques est désormais libéralisé, la mise à disposition du réseau et la mise en œuvre d'une connexion sur celui-ci n'est plus le fait d'un seul opérateur étatisé dit « historique » mais de différents opérateurs privés. La mise en œuvre du réseau internet et son accès n'ont jamais fait l'objet d'un monopole. Dès sa création se sont développés des opérateurs privés

[445] Ainsi en France l'ARCEP requiert depuis plusieurs années de Skype qu'elle se déclare en tant qu'opérateur pour que la société américaine soit soumise au régime notamment des appels d'urgence et des interceptions de sécurité (V. le communiqué de presse en date du 12 mars 2013 « Skype refuse de se déclarer en tant qu'opérateur », disponible sur le site www.arcep.fr) De fait l'Union européenne réfléchit actuellement à la rédaction d'un code européen des communications électroniques qui visera ces nouveaux services de l'Internet appelés les « OTT » pour « Over-the-top » (tels *Skype* mais également *Whatsapp*, *Hangouts*, *Viber* ou *Wechat*), v. le document de travail émis le 4 octobre 2016, « COMMISSION STAFF WORKING DOCUMENT Executive summary of the evaluation Accompanying the document proposal for a directive of the European Parliament and of the Council establishing the European Electronic Communication Code (Recast) », SWD (2016) 313 final, p.32 disponible sur eur-lex.europa.eu

[446] V. art L32, 3° CPCE.

[447] V. art L32, 4° CPCE.

[448] V. art L32, 5° CPCE.

qui souhaitaient fournir un accès à celui-ci aux particuliers ; ces opérateurs sont appelés dans le langage courant les « FAI » pour Fournisseurs d'Accès au Réseau.

La liste des opérateurs déclarés est publique et disponible sur le site de l'ARCEP ; en octobre 2016, l'autorité annonçait que le 2000ème opérateur s'était déclaré[449]. Ce chiffre est important et ne cesse d'augmenter alors que la logique de mise en œuvre de sous-réseaux toujours plus étendus oblige des collectivités à traiter directement avec le registre local pour obtenir une plage plus importante d'adresses IP à l'échelle du réseau mondial, et permettre dès lors des vitesses de transmission adéquates à la taille de leur parc de serveurs[450].

Ainsi une adresse IP renseigne sur un opérateur de communications électroniques, c'est-à-dire une entité qui met à disposition du public un accès physique à l'infrastructure du réseau mondial. Dès lors ce dernier est à même de localiser le point d'accès au réseau auquel il a attribué cette adresse[451] .

§2) La localisation d'un point d'accès au réseau permise par l'adresse IP

213. **La localisation du point d'accès au réseau.** Une adresse IP est un élément dit de « protocole » c'est-à-dire qu'elle traduit en langage numérique l'emplacement d'un point physique de connexion qui peut dès lors être localisé. Cette adresse révèle l'emplacement du terminal réalisant le point final de la boucle d'accès au réseau mondial, et éventuellement du terminal réalisant le point final de l'accès à un réseau local.

En effet un seul terminal, que ce soit une liaison filaire ou un point wifi ne peut opérer un nombre illimité de connexions. L'internet se présente comme une structure ramifiée qui met en œuvre des réseaux successifs. On distingue ainsi le réseau mondial et tous les points d'accès qui y sont reliés, des réseaux locaux mis en œuvre à partir de chacun de ces points.

Ainsi la logique de répartition des adresses IP sur le réseau s'opère en deux temps. D'abord un opérateur de communications électroniques adresse un point d'accès au réseau mondial. Cet adressage fait l'objet d'un contrat d'abonnement **(1).** Ensuite si un nombre important de connexions doivent être mises en œuvre à partir de ce point, un réseau local est créé. L'adressage de celui-ci permet de considérer la localisation

[449] Voir sur le site de l'ARCEP, la liste des opérateurs déclarés, onglet « opérateurs », www.arcep.fr
[450] La problématique est alors celle de la mise en œuvre d'une infrastructure qui relève du domaine public.
[451] A la différence d'une entreprise comme Skype qui achemine une communication mais ne voit se connecter à lui qu'une adresse IP et qui ne peut structurellement considérer le point d'accès qui la met en œuvre.

physique du dernier point d'accès au réseau qui nécessairement recouvre toujours un périmètre de connexion restreint **(2).**

A] L'accès au réseau, objet du contrat d'abonnement avec l'opérateur de communications électroniques

214. **L'objet du contrat d'abonnement.** Pour qu'un individu puisse se connecter au réseau, il doit disposer d'une adresse IP valide que lui attribue l'opérateur. Toutefois cette attribution ne peut se départir d'un accès au réseau de communication mondial qui matériellement doit transporter les paquets de données. Comme le souligne l'ARCEP : « *le fournisseur d'accès à Internet (FAI) gère les abonnements à Internet de ses clients et effectue la liaison avec un point d'échange de données d'Internet* »[452].

Ainsi l'objet du contrat d'abonnement est la mise en œuvre ou l'utilisation d'une boucle locale desservant le réseau mondial **(a)** qui va permettre la transmission des paquets IP **(b)**.

1) La mise à disposition d'une boucle physique d'accès au réseau

215. **L'accès à la structure du réseau**. L'opérateur de communications électroniques a structurellement accès au réseau. L'objet de son service est d'abord de mettre à disposition une boucle locale d'accès au réseau mondial.

Dans les premières années de mise en œuvre du réseau la problématique fût d'ailleurs de considérer comment ces nouveaux acteurs qu'étaient les opérateurs de communications électroniques pouvaient avoir accès au réseau de communication pour proposer leurs services et notamment s'agissant des FAI qui adressaient leurs offres aux particuliers. L'enjeu était pour ces derniers de pouvoir accéder à des infrastructures déjà existantes, notamment la boucle locale d'accès au domicile du particulier mis en œuvre par France Télécom alors que les connexions s'opéraient à l'origine via les câbles téléphoniques[453]. Aujourd'hui la multiplication de sous-réseaux étendus mis en œuvre par des collectivités et qui nécessitent un accès privilégié à la structure du réseau fait apparaître à une autre échelle la même problématique qui est celle de la mise en œuvre d'une infrastructure qui relève du domaine public.

[452] V. « L'accès à l'Internet, les entretiens de l'autorité, 18 janvier 2000 », document disponible sur le site de l'ARCEP, www. arcep.fr

[453] Il peut être rappelé qu'ainsi même si plusieurs FAI existent déjà à cette époque comme « Club Internet » par exemple et ont accès à ce réseau filaire pour mettre en œuvre leurs connexions, la majorité des utilisateurs ont souscrit un abonnement auprès de « Wanadoo » filiale de France Télécom, l'opérateur historique.

Aujourd'hui leur problématique est celle de la concurrence s'agissant du renouvellement du réseau, via des nouveaux modes de transmission comme la fibre, qui permettent des vitesses de transmissions plus rapides.

216. **Le coût de l'accès à la structure du réseau**. Une fois la structure filaire d'acheminement du signal mise en œuvre, les opérateurs de communications électroniques doivent permettre la communication. Ils doivent d'une part mettre à disposition des terminaux opérant le dernier point de connexion au réseau mondial. Pour un particulier, il s'agit de la « *box* » sur laquelle il peut brancher son ordinateur via un câble Ethernet mais qui permet aussi un signal en wifi.

Or tout point d'accès à l'internet est payant. La gratuité de l'usage de certains réseaux wifi comme ceux mis à disposition par exemple par des chaînes de restaurants ou des lieux publics ne doit pas masquer la réalité de l'utilisation d'une structure physique qui a un coût. A chaque point d'accès au réseau peuvent être associées les coordonnées bancaires d'un individu ou d'une société identifiée. Par exemple dans le cas d'un réseau domestique, le FAI établit un contrat d'abonnement qui facture les services dont il est prestataire. Le FAI connaît l'identité civile de son abonné. Les données à sa disposition peuvent être listées comme telles : *Contrat d'abonnement n°2402, Jean Dupont, 24 rue Monge, 75005 Paris, 2ème étage gauche (point de liaison du câble final), Relevé d'identité bancaire.*

Par ailleurs ces opérateurs de communications électroniques doivent d'autre part mettre en œuvre l'adressage de la connexion pour que les informations puissent transiter sur l'infrastructure mise à disposition.

2) L'attribution d'une adresse IP à chaque connexion au réseau

217. **La répartition dynamique ou statique des adresses IP à disposition de l'opérateur de communications électroniques**. L'attribution d'une adresse IP qui individualise[454] la connexion parmi toutes les autres connexions opérées en même temps, peut être mise en œuvre par l'opérateur de communications électroniques de manière statique ou dynamique.

En effet, alors que le nombre d'adresses IP n'est pas infini, l'opérateur peut ne pas disposer de suffisamment d'adresses différentes pour dissocier tous les points de connexion au réseau mondial qu'il souhaite mettre à disposition. Dès lors en considérant que tous ses terminaux ne sont pas connectés au même moment, il peut attribuer dynamiquement une adresse à l'un puis à l'autre pour des connexions qui se suivent dans le temps. Ainsi une adresse IP peut ne pas être associée de manière fixe à un point d'accès au réseau mondial.

[454] C'est-à-dire qu'elle la rend « *distincte des autres par des caractères propres* », V. l'entrée « individualiser » *in* Dictionnaire Le petit Larousse illustré 2015.

Toutefois, à cette échelle mondiale, le réseau grandissant, la logique aujourd'hui est de plus en plus celle de l'attribution à ces terminaux ou serveurs d'adresses IP fixes qui facilitent la vitesse de transmission.

218. **Les informations à dispositions de l'opérateur de communications électroniques**. Ainsi l'opérateur de communications électroniques est à même d'associer une adresse IP circulant sur le réseau avec le terminal auquel il l'a attribué, soit de manière fixe, soit le temps de la connexion s'il a opéré une répartition dynamique.

Le FAI est donc à même d'associer une adresse IP à une personne identifiée grâce aux informations qu'il détient s'agissant du titulaire de l'abonnement, notamment ses coordonnées. Mais surtout il est à même de renseigner que le point de liaison du câble final qui correspond à l'adresse IP, dessert le 2ème étage gauche de l'immeuble sis à cette adresse. Si cette nuance a peu d'incidence dans le cas d'un réseau peu étendu alors que la mention du nom et de l'adresse d'un particulier ou la dénomination d'un cybercafé va nécessairement renvoyer à la localisation du domicile ou du lieu où se situe le commerce, cette précision est utile quand l'adresse IP renvoie à l'abonnement d'une collectivité qui peut disposer de différents points d'accès en des lieux distincts. L'opérateur peut rendre compte de la dénomination de son client, comme l'Université Paris 2 Panthéon-Assas par exemple, mais surtout indiquer que l'adresse a été attribuée au serveur situé dans les locaux du 12 place du Panthéon. Ou encore l'opérateur peut indiquer que son cocontractant est la ville de Paris mais surtout dire qu'il s'agit de la borne wifi n°1 du jardin du Luxembourg.

Or il faut considérer que si ces boucles d'accès au réseau mondial doivent supporter un nombre trop important de connexions au même moment, il est nécessaire de mettre en œuvre à partir de ces points un nouveau réseau qui distribue à un niveau inférieur les connexions, ce qui permet de localiser physiquement une nouvelle boucle d'accès au réseau visant nécessairement un nombre limité de connexions.

B] Le lien entre une adresse IP et un périmètre de connexion restreint

219. **L'indication utile de l'adresse IP : le périmètre de connexion**. L'adresse IP renseigne donc sur la localisation physique d'un point d'accès au réseau. Autrement dit elle révèle l'emplacement de la machine réalisant le point final de la boucle d'accès au réseau mondial. Par ailleurs alors qu'un opérateur monnaie la mise en œuvre de cette boucle locale et entre donc dans une relation commerciale avec un tiers, que ce soit un particulier ou une entreprise, elle peut être associée aux coordonnées d'un abonné.

Disant cela le point de départ du procédé d'investigation permettant de considérer l'identité civile de l'internaute à l'origine de la connexion apparaît : l'adresse IP permet de localiser un point d'accès et dès lors de considérer l'individu qui a pu s'y connecter. L'erreur à ne pas commettre ici est de considérer que l'indication utile permise par l'adresse IP est l'identité du titulaire de l'abonnement. En effet il est évident que l'abonné n'est pas nécessairement l'individu à l'origine de la connexion, qui plus est quand ce titulaire est une personne morale, comme une entreprise ou une collectivité.

Ainsi l'indication clé permise par une adresse IP est la localisation physique d'un point d'accès au réseau.

220. **La problématique de la possibilité pour un point d'accès d'être utilisé par plusieurs individus**. Toutefois si l'adresse IP localise matériellement un terminal opérant un accès au réseau, que celui-ci soit filaire ou wifi, la problématique s'agissant de l'identification de l'internaute connecté est que ce point d'accès peut être utilisé par plusieurs personnes.

Or il faut souligner là encore que ce constat d'un public indéterminé ou étendu qui aurait accès à un point d'accès mis en œuvre par un abonné ne se fait de fait qu'au regard de la dénomination ou de l'activité du titulaire de l'abonnement. En réalité la problématique est celle de la localisation efficace d'un point d'accès, qui nécessairement recouvre une réalité physique. Or il va être vu que matériellement le champ d'investigation est toujours restreint alors que la structure physique du réseau nécessite un maillage qui conduit à multiplier les points d'accès au réseau. En effet un seul terminal ne peut opérer un nombre illimité de connexions. Ainsi la structure du réseau implique la mise en œuvre de réseaux locaux successifs qui viennent limiter le champ d'investigation à une boucle locale visant un espace géographique restreint.

221. ***Plan.*** Pour considérer le chemin menant d'une adresse IP visible sur le réseau jusqu'au point d'accès qui l'a émise dans le cas de la mise en œuvre d'un réseau local, il convient d'abord d'étudier le mécanisme d'adressage dit privé qui est mis en œuvre par ce sous-réseau **(a)** ce qui fait apparaître le rôle de l'administrateur réseau dans la localisation du point d'accès au réseau utilisé (**b).**

1) Le mécanisme d'adressage dit « privé » d'un réseau local

222. **Le maillage du réseau nécessaire à l'acheminement de la communication.** Toute machine connectée à partir d'un point d'accès au réseau mondial doit obtenir les réponses spécifiques à ses requêtes. Matériellement le chemin est celui-ci : le paquet IP demandé,

comme les informations d'un page web, doit se diriger vers la machine qui opère le point d'accès au réseau mondial, comme la « box internet » par exemple, elle doit ensuite être dirigée vers la machine connectée à ce point qui a émis la requête. Un point d'accès au réseau reconnait une nouvelle machine qui souhaite se connecter à lui grâce à l'adresse MAC de celle-ci qui est l'adresse propre de la machine déterminée par le constructeur[455]. Pour que cette machine ait accès au réseau une adresse spécifique doit lui être attribuée.

Le procédé d'adressage du réseau peut ainsi se comprendre en utilisant l'image de « poupées gigognes » ; le maillage du réseau est le fait de différents réseaux reliés entre eux qui sont adressés spécifiquement par ordre de taille.

223. **Deux niveaux d'adressages : adresses IP publiques et adresses IP privées** Ainsi le premier niveau d'adressage est celui du réseau mondial : tout accès au réseau doit avoir un identifiant unique mondialement. C'est cette adresse qui circule sur le réseau, elle est ainsi dite « publique ». Si plusieurs machines se connectent grâce à un même point d'accès un second niveau d'adressage se met en place. Chaque machine a une adresse unique dans le réseau local créé, adresse qui ne sera pas visible au niveau mondial et n'a donc pas à être unique à cette échelle : elle est ainsi dite « privée ».

Ce second niveau d'adressage à partir d'un certain seuil de connexions ne peut plus se faire automatiquement. En effet un point de liaison ne peut supporter qu'un débit limité et ne peut hiérarchiser un nombre trop important de connexions. Il y a ce qu'on appelle un conflit d'adresses IP : les informations arrivent jusqu'au point d'accès connecté au réseau mondial mais sont bloquées ne sachant pas vers quel ordinateur aller.

Il est alors nécessaire de mettre en œuvre un sous-réseau, dit aussi « réseau local », qu'il faut administrer pour organiser la transmission des informations entre les nouveaux points de liaisons créés.

2) Le rôle de l'administrateur réseau.

224. **La fonction de l'administrateur**. Le terme « administrateur » est révélateur de l'enjeu de sa fonction ; il n'intervient pas dans la conception de l'architecture du sous-réseau aidé en cela par un architecte réseau, il gère celui-ci[456]. Ainsi l'administrateur réseau « *n'a pas besoin d'être un génie de la technique. En fait quelques uns des meilleurs administrateurs*

[455] Cette adresse obéit ainsi à la même logique que l'adressage du réseau puisqu'il faut pouvoir identifier de manière unique chaque machine construite. Toutefois cet adressage intervient à un niveau qui n'est pas visible sur le réseau mondial. Les adresses MAC ne circulent pas sur le réseau mais permettent techniquement la mise en œuvre de sous-réseaux. De plus il faut bien souligner que si elles permettent de dissocier les machines les unes des autres, en aucun cas un lien ne peut être fait avec l'acheteur de la machine

[456] Voir l'entrée « administrateur réseau » sur le site wikipédia.org

réseau se révèlent être dénués de toutes connaissances techniques. Ce qui est important c'est que l'administrateur réseau soit bien organisé. »[457]. Il doit en effet organiser l'accès au réseau de plusieurs milliers de connexions. Il doit veiller notamment au bon routage[458] des informations, gérer l'espace libre sur les serveurs du réseau, garantir la sauvegarde et la sécurité des données échangées et enfin mettre en œuvre une politique quant à l'attribution d'une adresse IP privée permettant une connexion au réseau mondial[459]. C'est ainsi lui qui est à même par la mise en œuvre de fichiers complexes, dits « fichiers traces », de considérer à quelle adresse IP privée renvoie une adresse IP publique qui a opéré une connexion sur le réseau mondial.

225. **Le lien entre une adresse IP et un périmètre d'investigation efficace**. Ainsi cet acteur de tout réseau local étendu va pouvoir considérer que l'adresse IP publique litigieuse émise par le serveur installé dans les locaux du 12 place du Panthéon qui fait l'objet d'un abonnement avec un opérateur, correspond à l'adresse IP privée allouée par exemple à la borne Wifi du 2ème étage de l'aile Cujas du bâtiment Panthéon, ou qu'il s'agit du poste du secrétariat du CEJEM.

Ainsi une adresse IP renvoie toujours à un lieu physique de connexion qui est restreint, en ce sens qu'il correspond à une prise filaire ou à un terminal émettant un signal wifi d'une portée de quelques mètres. Le champ d'investigation s'agissant de l'internaute à l'origine de la connexion devient efficace. Quand bien même le public qui a accès au réseau peut être indéterminé, la personne à l'origine de la connexion était présente à cet endroit précis à l'heure de celle-ci.

Ainsi une adresse IP renvoie à une connexion unique à un moment « t » donné et à un espace géographique restreint de connexion. Elle peut être rattachée dans le cadre du fichier mis en œuvre par l'opérateur de communications électroniques à un abonné et surtout à la localisation de son point d'accès. Elle permet dès lors par un procédé d'investigation d'identifier l'internaute connecté.

[457] LOWE Doug, *Créer son réseau pour les nuls*, Paris, 2010 : Editions First, p.19.

[458]« Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. »,voir l'entrée « routage » sur le site wikipédia.org.

[459] « On désigne par le terme administration-la gestion des utilisateurs et de la sécurité- la mise à disposition des ressources- la maintenance des applications et des données –l'installation et la mise à niveau des logiciels utilisateurs », PILLOU Jean-François, Tout sur les réseaux, 3ème éd., Paris : DUNOD, 2012 (Commentçamarche.net), p. 9.

Section II. Les inconvénients de la qualification de l'adresse IP en tant que donnée à caractère personnel

226. **Le consensus originel sur le caractère indirectement nominatif de l'adresse IP.** Une adresse IP est reliée à un abonné et il n'est pas de problématique à l'origine sur son caractère indirectement nominatif eu égard aux conditions d'accès au fichier mis en œuvre par le FAI.

Ainsi en 1998 dans son étude intitulée « *Internet et les réseaux numériques* » l'Assemblée générale du Conseil d'État affirme que bien qu'il n'existe pas de jurisprudence sur la nature des données de connexion à un site internet, il ne fait toutefois aucun doute que ces données de connexion, adresse IP et données associées, sont indirectement nominatives « *dans la mesure où le fournisseur d'accès peut associer le nom d'un client à une adresse IP* »[460]. De la même manière le Groupe de l'article 29 dans un avis adopté en 2000 soutient que « *les fournisseurs d'accès internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs internet auxquels ils ont attribué ces adresses […] Il en va de même pour les fournisseurs de services internet qui conservent un fichier registre sur le serveur HTTP. Dans ces cas on peut parler sans l'ombre d'un doute de données à caractère personnel au sens de l'article 2, point a), de la directive* »[461].

En effet la logique de l'indirectement nominatif sied parfaitement à l'adresse IP : ce numéro ne permet pas d'accéder directement à l'identité réelle de l'intéressé, à savoir l'abonné, à l'inverse d'un nom ou de coordonnées. Il ne le peut qu'après un rapprochement avec les données détenues par les opérateurs techniques. Il est courant alors d'opérer une comparaison avec le numéro de téléphone ou la plaque d'immatriculation d'un véhicule[462].

227. **Le contentieux de la recherche de l'auteur d'une infraction.** Toutefois le contexte de la lutte contre le téléchargement illégal via les sites de P2P dans les années 2010 va venir

[460] *Internet et les réseaux numériques*, étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998, (Collection études du Conseil d'État), p.34.

[461] Avis 34/2000 du Groupe « article 29 » sur le « Le respect de la vie privée sur internet- une approche européenne sur la protection des données en ligne», novembre 2000, WP 37.

[462] « L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes », Avis CNIL mis en ligne sur son site le 2 Août 2007. V. : P. LECLERQ, « Un d'application de la législation" informatique et libertés " », Chronique « un an de … », *CCE*, octobre 2007, p. 27 ; C. CARON, « Qualification de l'adresse "IP" : état des lieux jurisprudentiel », *CCE*, décembre 2007, *comm.* 144 ; « Entretien avec Yann Padova, secrétaire général de la CNIL », *Gaz. Pal.* N°15 du 15 janvier 2008, p.2. V. également : CNIL, « Délibération n°2006-294 du 21 décembre 2006 » qui autorise l'ALPA à mettre en œuvre un traitement de données à caractère personnel ayant pour finalité principale la recherche des auteurs des contrefaçons audiovisuelles, p. 3.

faire apparaître la problématique de la qualification de l'adresse IP en tant que donnée à caractère personnel.

D'une part d'abord on s'interroge sur le lien d'une telle adresse avec l'auteur de l'infraction qui n'est pas nécessairement le titulaire de l'abonnement. Par un raccourci critiquable, il est souvent affirmé alors que le numéro IP ne correspond qu'à une machine. Si cette affirmation est techniquement très imprécise[463], elle renvoie davantage au phénomène de la multiplication dans les années 2000 des cybercafés puis par la suite des points de connexion mis à disposition en wifi. En réalité le contrefacteur n'est jamais identifié automatiquement par son adresse IP et ne peut être retrouvé que par la mise en œuvre d'une investigation. Or cette investigation n'est pas nécessairement vouée à l'échec dans le cas d'un point d'accès au réseau utilisé par un public indéterminé alors que le périmètre physique de connexion est nécessairement restreint[464].

Ainsi d'autre part et par la suite, l'enjeu n'est plus celui du potentiel d'identification de la personne grâce à l'adresse IP mais celui des conditions de cette identification. Si l'adresse IP est bien une donnée personnelle pour le FAI alors que par le truchement du traitement opéré par son fichier elle permet une identification automatique de l'abonné, l'est-t-elle pour toute personne qui la visualise sur un site de P2P et qui, si elle peut être responsable d'un traitement, n'a pas à sa disposition les coordonnées de l'abonné.

228. ***Plan.*** Ainsi le contexte de la lutte contre le téléchargement illégal fait apparaître une nouvelle problématique : l'adresse IP visible sur le réseau est-elle en soi une donnée personnelle eu égard à son potentiel d'identification et toute personne la collectant opère-t-elle alors un traitement de données à caractère personnel ? Les juges du fond sont partagés **(§1).** La CJUE et la Cour de cassation française vont venir affirmer que l'adresse IP est une donnée personnelle suivant en cela le mouvement d'objectivisation du champ d'application de la loi Informatique et Libertés. Une position qui n'est pas exempte de toute critique alors qu'aucune donnée ne peut être personnelle en soi **(§2).**

[463] V. *supra* section I : « *Le fonctionnement de l'adressage du réseau* ».

[464] Au contraire, dès cette époque, on peut ainsi déjà affirmer qu'il est facile de remonter à l'adresse IP d'un cybercafé puisque le ou les serveurs de celui-ci qui doivent supporter un nombre important de connexions sont dotés d'une adresse IP fixe.

§1) Le débat entourant la qualification de l'adresse IP dans le contexte de la lutte contre le téléchargement illégal

229. **Le contexte de la lutte contre le téléchargement illégal**. Le débat entourant la qualification de l'adresse IP a vu le jour dans le cadre de la lutte contre le téléchargement illégal. En effet les sociétés de perception de droits devant l'ampleur que prennent au milieu des années 2000 les réseaux de P2P[465], permettant d'échanger à l'échelle mondiale très facilement des fichiers, souhaitent pouvoir identifier l'internaute-contrefacteur qui met donc à disposition un fichier dont il ne détient pas les droits. Elles souhaitent mettre en œuvre des logiciels permettant d'enregistrer les adresses IP visibles publiquement sur ces réseaux et ce, à fin d'avertir l'internaute contrefacteur et le cas échéant d'intenter à son encontre des poursuites pénales[466]. Ces traitements sous couvert de l'ancienne mouture de la loi Informatique et Libertés sont soustraits au contrôle a priori de la CNIL alors qu'ils sont mis en œuvre par des personnes privées ; toutefois l'autorité administrative considère que de telles collectes de données qui visent la constatation d'infractions sont contraires à la loi et ne doivent pas être mis en œuvre[467].

La nouvelle rédaction issue de la loi du 6 Août 2004 clarifie la situation en autorisant de tels traitements de données à caractère personnel qui visent spécifiquement la constatation d'infractions aux droits garantis par la première partie du Code de la propriété intellectuelle[468]. Ces traitements doivent être autorisés par la CNIL[469]. A

---

[465] Le « *P2P* », acronyme de « *Peer-to-Peer* » que l'on pourrait traduire en français par « *pair-à-pair* » ou « *poste-à-poste* » est un modèle de réseau informatique qui se différencie du modèle « client-serveur ». Dans un réseau P2P, tout poste est à la fois client et serveur, ce qui fait que les nœuds d'échanges sont multipliés ce qui permet de faciliter le partage d'informations. Grâce à cette technique, les internautes peuvent ainsi mettre à disposition des fichiers, ou une partie de la puissance de calcul de leur machine ou encore une partie de leur débit pour la mise en œuvre de certains services. V. pour une définition l'entrée « Pair-à-pair » sur le site *wikipédia.org*.

Napster est le premier logiciel de ce type, il a été lancé en 1999 par Shawn Fanning, informaticien âgé de 18 ans, alors encore étudiant à la Northeastern university de Boston. Napster a fermé en 2002 sur injonction des autorités américaines. V. pour un historique de la création de Napster, le site numerama.com et son article sur l'histoire du peer-to-peer, disponible à cette adresse : http://www.numerama.com/magazine/d/2/8002-L-Histoire-du-peer-to-peer.html

[466] Dès 2001, les ayant-droits et leurs représentants avouent avoir recours à des applications leur permettant de détecter les fraudeurs, applications encore en phase de test. Tout reste flou : la technique utilisée, les cibles de la surveillance - l'utilisateur ou les sites ou logiciels pirates-, les données collectées. Ainsi, Marcel Heymans, le responsable de la filière belge de l'IFPI (Fédération Internationale de l'Industrie Phonographique) dès février 2001, indique que son organisation dispose d'équipements de détection permettant de localiser par milliers les utilisateurs fraudeurs. Les internautes belges, utilisateurs de Napster peuvent alors recevoir des mails de leur FAI rédigés par l'IFPI qui leur rappellent les lois sur le droit d'auteur et la propriété intellectuelle. V. : GUILLEMIN Christophe, « L'arme de surveillance contre les utilisateurs de Napster » Zdnet.fr, publié le 5 avril 2001

[467] Sous l'empire de l'article 16 de l'ancienne loi Informatique et Libertés, une société de gestion de droit (la SDRM) déclare la mise en œuvre d'un traitement d'adresses IP via un logiciel de contrôle spécifique des réseaux P2P, appelé « Webcontrol ». La CNIL, alors que le dossier est complet, remet le récépissé de déclaration mais indique dans un courrier que les caractéristiques du traitement lui paraissent contraires aux dispositions de la loi alors qu'un tel logiciel permettrait de constituer des fichiers nominatifs concernant des infractions, ce qu'interdit l'article 30 de la loi du 6 janvier 1978. L'autorité administrative indique que ce traitement est de nature à exposer la société aux sanctions pénales prévues par l'article 42 de la loi du 6 janvier 1978 non encore modifiée. V. la saisine du Conseil constitutionnel en date du 20 juillet 2004 par plus de 60 députés, qui fait état d'un courrier de la CNIL en date du 15 mars 2001 relatant de la position de la CNIL quant à la mise en œuvre de ce logiciel et du traitement qu'il permet, NOR CSCL0407511X, JORF Août 2004, p.14090.

[468] Article 9, 3° de la loi du 6 janvier 1978 telle que modifiée par la loi n°2004-801 du 6 Août 2004, JORF du 7 Août 2004, texte 2 sur 92. Le traitement ne peut être mis en œuvre que par « Les personnes morales mentionnées aux articles L.

l'origine le raisonnement même s'il n'est pas exempt de critiques, est clair, comme en témoigne la décision du Conseil constitutionnel : les adresses IP sont des données personnelles qui peuvent être reliées à un individu identifié et leur collecte doit être soumise à autorisation de la CNIL. Le traitement de telles données par les sociétés de perception de droits ne porte pas atteinte aux droits et libertés de l'individu puisque ces traitements sont circonscrits et que les adresses collectées ne peuvent obtenir de caractère nominatif que si des poursuites sont mises en œuvre. Autrement dit le traitement effectué par les sociétés de perception de droits ne permet pas une identification automatique de l'abonné et encore moins de l'internaute connecté[470].

230. **La problématique de la surveillance automatisée des réseaux P2P avant la création de la HADOPI.** Toutefois la CNIL éprouve des difficultés à autoriser certains systèmes de collecte, qui, alors que les mécanismes de l'HADOPI ne sont pas encore mis en œuvre s'agissant de ce phénomène de masse, sont le fait d'organismes privés qui visent une surveillance de grande ampleur du réseau et des internautes[471]. Si ces décisions de refus sont annulées par le Conseil d'État[472], la problématique s'agissant de la nature de l'adresse IP subsiste.

321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits. ».

[469] Article 25, I, 3° de la loi du 6 janvier 1978 telle que modifiée par la loi n°2004-801 du 6 Août 2004, JORF du 7 Août 2004, texte 2 sur 92.

[470] Cons. Const., déc. n°2004-499 DC du 29 juillet 2004, loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi du 6 janvier 1978 relative à l'informatique au fichiers et aux libertés, JORF du 7 Août 2004, texte 9 sur 92, considérant 13.

[471] V. Quatre délibérations de la CNIL en date du 18 octobre 2005, portant refus d'autorisation de la mise en œuvre « d'un traitement de données à caractère personnel ayant pour finalités, d'une part, la constatation des délits de contrefaçon commis via les réseaux d'échanges de fichiers dénommés « peer-to-peer », d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en manière de contrefaçon » ; délibération n°2005-235 (visant la SACEM), délibération n°2005-236 (visant la SCPP), délibération n°2005-237 (visant la SPPF) et la délibération n°2005-238 (visant la SDRM), disponibles sur le site de la CNIL. L'autorité administrative soutient que les traitements de ces organismes « ne sont pas proportionnés à la finalité poursuivie dans la mesure où ils n'ont pas pour objet de permettre la réalisation d'actions ponctuelles strictement limitées aux besoins de la lutte contre la contrefaçon mais peuvent aboutir au contraire à une collecte massive de données à caractère personnel sur internet et à une surveillance exhaustive et continue des réseaux d'échanges de fichiers dénommées « peer-to-peer ».

A l'inverse dans deux autres délibérations en date du 24 mars 2005 et du 21 décembre 2006 (Délibération n°2005-050, visant le SELL, et la délibération 2006-294 visant l'ALPA, disponibles sur le site de la CNIL), elle conclue à la proportionnalité du traitement mis en œuvre vis-à-vis des finalités de lutte contre la contrefaçon. Ce que condamne donc la CNIL est l'automatisme de la surveillance du réseau qui doit être circonscrite à des actions ponctuelles. Il est à noter que dans un arrêt du 4 avril 2007, la Cour de cassation est amenée à se prononcer sur le fichier mis en œuvre par le SELL qui a été autorisé par la CNIL ; elle énonce que « *les garanties qui accompagnaient sa mise en œuvre étaient de nature à préserver l'équilibre entre la protection des droits reconnus aux personnes dont les données sont traitées et la protection des droits dont bénéficient les auteurs et leurs ayants droit* » et dès lors considère que les autorisations de la CNIL opèrent validation rétroactive du traitement mis en œuvre. V. : Ccass. Crim, 4 avril 2007, RG n° 07-80267.

[472] CE, 23 mai 2007, n°288149, SACEM et al., Juris-Data n°2007-071900.Les conclusions du commissaire du gouvernement Célia Vérot ont été suivies, v. *AJDA,* 16 juillet 2007, p. 1413. Il y a une erreur d'appréciation de la CNIL qui doit pour considérer la proportionnalité du traitement envisager l'ampleur du phénomène de contrefaçon sur l'Internet. Il est rappelé que la loi Informatique et Libertés a été modifiée pour permettre l'automatisation à cette fin de la surveillance des réseaux P2P. En revanche n'est pas censurée l'argument de la CNIL qui conduit à interdire la fonctionnalité d'envoi de messages aux

En effet, alors que le débat est vif s'agissant de la mise en œuvre par des sociétés privées de procédés automatiques de fichage des adresses IP en vue de la constatation d'infractions, il est par ailleurs procédé à l'identification du contrefacteur sans passer par ces traitements. Les organismes de défense des ayants-droit vont en effet faire appel à des agents assermentés qui relèvent les adresses une par une pour ensuite mettre en œuvre des poursuites. Par le biais du « *simple constat* » les sociétés entendent se soustraire à l'autorisation de la CNIL alors qu'il n'y a pas de traitements automatisés de données personnelles. Un contentieux nouveau apparaît s'agissant de la nécessité ou non de demander l'autorisation de la CNIL pour mettre en œuvre ces constats qui questionnent non seulement la nature personnelle de l'adresse IP mais également la notion de traitement.

De fait les deux qualifications sont rarement dissociées : soit les juges du fond concluent à la nature personnelle de la donnée et à la nature automatisé du traitement, soit ils concluent à l'inverse à l'absence de ces deux critères d'application de la loi Informatique et Libertés (**1**). La Cour de cassation en 2009 opère une analyse originale alors qu'elle dissocie ces deux critères ; elle ne met toutefois pas fin aux doutes concernant la qualification de l'adresse IP alors que si elle affirme qu'il n'y a pas de traitement automatisé en l'espèce, elle ne se prononce pas sur la nature personnelle de l'adresse IP (**2**).

A] La divergence de position des juridictions du fond

231. **Le contentieux visant les constats d'agents assermentés relevant une adresse IP sur les réseaux P2P.** Les affaires soumises au juge judiciaire sont similaires dans leurs faits. Les actions sont à l'initiative des sociétés de perception et de répartition des droits définies à l'alinéa premier de l'article L321-1 du CPI et qui ont qualité pour ester en justice au titre de l'article L321-2 de ce même code. Elles agissent au pénal pour voir punie l'infraction de contrefaçon réalisée par la mise à disposition d'œuvres protégées grâce à un logiciel de P2P.

En amont de l'instance, un agent assermenté au titre de la mission qui lui incombe selon l'article L331-2 du CPI a lancé sur un réseau P2P une requête portant sur des titres appartenant au catalogue de la société qui l'emploie pour repérer un utilisateur

---

contrefacteurs par le biais du FAI. Quand bien même les sociétés de défense des droits d'auteur ne sont pas à même de connaître l'identité de l'abonné au réseau, cette identification ne peut être mise en œuvre par le FAI en dehors de toute procédure judiciaire.

Suite à l'annulation partielle du Conseil d'Etat, la CNIL, par deux décisions en date des 8 et 22 novembre 2007 va autoriser les quatre sociétés de perception et de répartition des droits d'auteur à mettre en œuvre leurs traitements, qui ne prévoient plus d'envoi automatique de messages aux internautes

qui met à disposition en nombre[473] ces fichiers. Les informations à sa disposition sont un pseudonyme et une adresse IP qui est souvent visible publiquement sur ces réseaux d'échanges ; à défaut un logiciel spécifique permet d'extraire l'adresse en question[474]. Un autre logiciel, disponible à tous, permet ensuite de relier cette adresse à un FAI[475]. Un constat est dressé relevant l'élément matériel de l'infraction ainsi que l'adresse IP et le FAI associé à cet acte.

La société de gestion collective porte alors plainte contre X auprès des services de police ou de gendarmerie et produit le constat ; le procureur de la République informé de la commission d'une infraction autorise, dans le cadre de l'enquête préliminaire, les officiers de police judiciaires à adresser aux FAI une réquisition afin d'obtenir les coordonnées de l'abonné au titre de l'article L34-1 II du CPCE. Les officiers de police entrent alors en contact avec l'abonné et par des investigations simples découvrent qui est l'auteur de l'infraction[476]. En l'état dès lors du dossier de procédure[477], des poursuites pénales peuvent être engagées[478].

Toutefois le prévenu va alors arguer de la nullité du constat de l'agent assermenté dès lors que selon lui ce constat est un traitement de données personnelles qui doit être soumis à l'autorisation de la CNIL alors qu'il vise la constatation d'une infraction. Si l'autorisation fait défaut, le constat est nul, ce qui a pour effet de vicier les actes de procédure subséquents.

232. **La problématique du champ d'application élargi de la loi Informatique et Libertés.** A l'origine des décisions de premières instances rejettent l'exception de nullité de la

[473] Il est en effet à noter que les poursuites vont être engagées dès lors que ce nombre est grand et ce pour que l'action permette une indemnisation efficace des sociétés de gestion collective et donc des ayant-droits. Voir les faits dans l'arrêt de la Cour d'Appel de Paris du 29 janvier 2008 (13ème ch. Section A.) et les faits dans le jugement du tribunal de grande-instance de Saint-Brieuc du 6 septembre 2009 : plus de 12 000 titres musicaux étaient à disposition dans la première affaire, plus de 140 000 dans la seconde. Il est également à noter que dans le cadre de ce contentieux des échanges de fichiers permis par les réseaux P2P, les contrefacteurs les premiers inquiétés sont ceux qui mettent à disposition et non ceux qui téléchargent alors que les fonctionnalités de ces outils d'échange ne permettent pas de voir le nombre de téléchargement à l'actif de chaque utilisateur mais listent en revanche le nombre de fichiers mis à disposition.

[474] Voir les faits dans le jugement du tribunal de grande-instance de Saint-Brieuc du 6 septembre 2009, l'agent assermenté utilise le logiciel « *Kerio personnal firewall* ». Voir également les faits de l'arrêt de la Cour d'appel de Rennes du 23 juin 2008, l'agent utilise le logiciel « *Spyster* » pour extraire l'adresse IP de l'internaute.

[475] Voir les faits dans l'arrêt de la Cour d'Appel de Paris du 29 janvier 2008 (13ème ch. Section A.) et les faits dans le jugement du tribunal de grande-instance de Saint-Brieuc du 6 septembre 2009 : dans les deux espèces, l'agent assermenté utilise le logiciel « *Visual route* » « *librement accessible par l'internet* », pour relier l'adresse IP aux fournisseurs d'accès à internet, Free dans la première espèce et Wanadoo dans la seconde. Peut être également cité le site internet "ripe.net" qui donne accès à la base de données "*Whois"* et indique le nom du FAI associé à toute adresse IP.

[476] Les OPJ se rendent au domicile de l'abonné, entendent celui-ci et procèdent aux perquisitions nécessaires. Il arrive souvent que le titulaire de l'abonnement ne soit pas le contrefacteur mais des mesures d' investigation simple auprès de l'abonné permettent de découvrir qui est l'auteur des faits présent au moment de la connexion litigieuse : le concubin de l'abonné par exemple ou un colocataire occasionnel.

[477] L'auteur présumé des faits est identifié, un complément d'enquête n'est pas nécessaire et à fortiori une instruction.

[478] Le contrefacteur présumé est cité devant la juridiction de jugement par le ministère public ; la société de gestion collective à l'origine de la plainte se constitue alors partie civile par la voie de l'intervention.

procédure sans prendre, et ce avec bon sens, de position sur le caractère personnel de l'adresse IP. Une donnée n'est jamais personnelle en soi mais l'est au regard d'un traitement qui automatiquement la rattache à un individu identifié. Or ici il est conclu que seule l'exploitation de la donnée par un officier de police judiciaire a permis d'identifier l'internaute mais que jamais cette donnée à disposition de l'agent assermenté ne lui a permis de découvrir automatiquement les coordonnées de l'abonné, et encore moins l'identité de l'internaute connecté[479].

Toutefois cette approche ne correspond pas à l'évolution de l'appréciation des critères de la loi Informatique et Libertés. La nature personnelle d'une donnée renvoie aujourd'hui au potentiel d'identification de celle-ci. Et la notion de traitement tend à se confondre avec celle de numérisation. Ainsi le problème de droit posé par ce contentieux n'est pas celui de la possibilité pour l'agent assermenté d'identifier automatiquement l'internaute mais celui de savoir si une adresse IP peut conduire à l'identification d'un internaute et si l'agent assermenté réalise le traitement d'une telle donnée. Alors que le caractère personnel d'une donnée ne s'envisage plus au regard des conditions de son traitement, les juridictions pénales vont nécessairement diverger sur la nature personnelle ou non de l'adresse IP, qui dans l'absolu permet d'identifier le contrefacteur mais qui ne le permet pas automatiquement pour l'agent assermenté, et sur la notion de traitement alors qu'une adresse IP est nécessairement une donnée produite automatiquement par le réseau.

233. ***Plan.*** Ainsi plusieurs décisions de première instance concluent à la nature personnelle de l'adresse IP **(a)** alors que pour sa part la Cour d'appel de Paris lui dénie cette qualification **(b)**.

1) Les décisions concluant à la nature personnelle de l'adresse IP

234. **Le raisonnement original du Tribunal de grande instance de Montpellier en 2006.** En 2006, une décision peu commentée du Tribunal de grande instance de Montpellier opère un raisonnement original s'agissant de l'application de la loi informatique et Libertés aux opérations mises en œuvre par l'agent assermenté en énonçant que « *Si l'adresse peut légitimement être considérée comme une donnée à caractère personnel au sens de la loi du 6 janvier 1978, les constatations opérées par l'agent assermenté excluent tout traitement au*

[479] V. : TGI Montauban, jugement du 9 mars 2007, RG n°396/2007. Décision citée par Maître Lucien Flament, v. : FLAMENT Lucien, « Le numéro d'IP n'est pas une donnée à caractère personnel-La cour d'appel de Paris persiste et signe ! », *Droit Pénal*, n°12, décembre 2008, étude 27.

sens de ce même texte, seul un officier de police judiciaire ayant traité cette donnée personnelle en requérant le fournisseur d'accès »[480]. Ainsi l'identification automatique de l'abonné à partir du numéro IP n'est pas et ne peut pas être le fait de l'agent assermenté ; le traitement permettant l'identification est mis en œuvre par les officiers de police judiciaire qui seuls peuvent interroger le fichier du FAI. Toutefois cette nuance ne va par la suite plus être faite par les juridictions du fond qui concluent à la nature personnelle de l'adresse IP et à son traitement par l'agent assermenté qui a utilisé deux logiciels, un pour extraire l'adresse IP et un autre pour obtenir à partir de celle-ci les coordonnées du FAI.

235. **Les décisions remarquées en 2006 et 2007 des Tribunaux de grande instance de Bobigny et Saint-Brieuc et de la Cour d'appel de Rennes**. Deux décisions de première instance remarquées en 2006[481] et 2007[482] concluent à la qualification de l'adresse IP comme donnée à caractère personnel en ces termes : « *L'adresse IP est au sens strict l'identifiant d'une machine lorsque celle-ci se connecte sur internet et non d'une personne. Mais au même titre qu'un numéro de téléphone n'est, au sens strict, que celui d'une ligne déterminée pour laquelle un abonnement a été souscrit par une personne déterminée ; un numéro IP associé à un fournisseur d'accès correspond nécessairement à la connexion d'un ordinateur pour lequel une personne a souscrit un abonnement auprès de ce fournisseur d'accès. L'adresse IP de la connexion associée au fournisseur d'accès constituent un ensemble de moyens permettant de connaître le nom de l'utilisateur »*[483]. La Cour d'appel de Rennes énonce de la même manière que l'adresse IP est une donnée indirectement nominative « *qui acquiert ce caractère nominatif par le simple rapprochement avec la base de données détenue par le FAI* »[484]. Des conclusions qui appliquent justement la loi Informatique et Libertés qui vise une donnée pouvant être reliée à un individu identifié ou identifiable, et de fait l'adresse IP permet de connaître le nom de l'abonné et de remonter au contrefacteur.

En revanche sur l'appréciation d'un traitement automatisé au regard de la seule nature informatique des procédés utilisés, le raisonnement paraît spécieux. Les juges

[480] TGI Montpellier, 20 nov. 2006, RG n°06/3865. Décision citée par Maître Lucien Flament, v. : FLAMENT Lucien, « Le numéro d'IP n'est pas une donnée à caractère personnel-La cour d'appel de Paris persiste et signe ! », *Droit Pénal*, n°12, décembre 2008, étude 27.

[481] TGI Bobigny, 15ème ch., 14 décembre 2006, « L'adresse IP constitue une donnée à caractère personnel en ce qu'elle permet d'identifier une personne en indiquant sans doute possible un ordinateur précis. Le numéro IP établit la correspondance entre l'identifiant attribué lors de la connexion à l'internaute et l'identité de l'abonné ».

[482] TGI St-Brieuc, 6 septembre 2007, nº 05003922, Ministère public et SCPP c/ M. J. P, Juris-data : 2007/349373, V. *RLDI* 2007, n°31, point 29, *observations* ; CARON Ch. « Qualification de l'adresse « IP » : état des lieux jurisprudentiel », Comm. Com. Electr.2007 n°12, comm. 144.

[483] Ibid.

[484] CA Rennes, 3ème ch. Corr., 22 mai 2008, RG n°07/01495, C.S. c/Sacem ; CA Rennes 3ème ch. Corr, 23 juin 2008 , T.L. c/SCPP ; CA Rennes, 3ème ch. Corr ,11 décembre 2008. V. : *Gaz. Pal, 23/24 janvier 2009*, jurisprudence, p.40, note NADEAU A., ROQUEFEUIL (de) B. ; DROUARD E., BLANCHARD M., « L'adresse IP est-elle une donnée personnelle ? », *Légipresse*, n°255, octobre 2008, p.185.

énoncent en effet qu'alors qu'un logiciel est utilisé pour extraire l'adresse IP et obtenir les coordonnées du FAI, il y a traitement automatisé alors qu' « *un programme informatique qui comporte une suite d'instructions s'exécutant par enchaînements successifs jusqu'au terme prévu est un processus automatisé* »[485]. Or cette argument a peu de sens alors que ce que cherchait à encadrer la loi Informatique et Libertés à l'origine était l'identification automatique de l'internaute via un procédé informatique et non le traitement automatique d'une donnée en lui-même. Apparait ici le caractère pervers du contentieux[486] alors que le juge n'appréhende pas correctement les enjeux d'identification de l'internaute via l'adresse IP mais considère le caractère automatique ou non de procédés visant la surveillance du réseau pour lutter contre le téléchargement illégal.

2) La position inverse soutenue par la Cour d'appel de Paris

236. **La position inverse soutenue par la Cour d'appel de Paris**. De fait la Cour d'appel de Paris va elle tenir le raisonnement inverse en vue de valider les poursuites permettant de sanctionner un contrefacteur[487].

Elle énonce que l'adresse IP est une « série de chiffres qui ne constitue en rien une donnée indirectement nominative relative à une personne dans la mesure où elle se rapporte à une machine et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon »[488] ce qui peut être critiqué alors que cette donnée est l'identifiant indirect d'un abonné par le truchement du fichier du FAI et constitue alors le point de départ efficace s'agissant d'une investigation visant l'identification du contrefacteur. Plus justement en revanche elle énonce qu'il n'y a pas de traitement de données à caractère

[485] TGI St-Brieuc, 6 septembre 2007, *op. cit*. Dans le même sens v. : Rennes, 3ème ch. Corr., 22 mai 2008, RG n°07/01495.

[486] CARON Ch. « Qualification de l'adresse « IP » : état des lieux jurisprudentiel *op. cit.*

[487] CA Paris, 27 avril 2007, 13e ch. Section B, RG n°06/02334, JurisData n°2007-338935 ; CA Paris, 15 mai 2007, 13e ch. section A, RG n°06/01954, JurisData n°2007-336454; CA Paris 29 janvier 2008, 13e ch. section A, RG n°07/05373, JurisData n°2008-355382. V. la position du professeur Ch. Caron qui énonce justement que «*Traditionnellement il est admis que l'adresse IP est une donnée indirectement nominative au sens de l'article 2, alinéa 2, de la loi «Informatique et Libertés» du 6 janvier 1978. Mais, afin d'éviter que les constats soient contestés sur ce fondement, un courant jurisprudentiel tend à considérer que l'adresse IP n'est pas une donnée personnelle*" et qu' "*En définitive la cour d'appel de Paris refuse que la législation "informatique et libertés" puisse avoir une influence sur la mise en œuvre des règles propres au droit d'auteur et aux droits voisins, ce qui revient à cultiver une certaine autonomie de ces disciplines afin de les rendre plus efficaces*", CARON Ch., *Droit d'auteur et droits voisins*, LexisNexis Litec, 5ème éd., 2017, n°.540 (Manuel), et CARON Ch. « Qualification de l'adresse « IP » : état des lieux jurisprudentiel », *Comm. Com. Electr*.2007 n°12, *comm.* 144. V. Également l'étude de Lucien Flament qui souligne que "*La spécificité de l'action pénale explique largement cette importante divergence de vues*", FLAMENT Lucien, « Le numéro d'IP n'est pas une donnée à caractère personnel-La cour d'appel de Paris persiste et signe ! », *Droit Pénal*, n°12, décembre 2008, étude 27.

[488] CA Paris, 15 mai 2007, 13e ch. section A, RG n°06/01954, JurisData n°2007-336454; CA Paris 29 janvier 2008, 13e ch. section A, RG n°07/05373, JurisData n°2008-355382. La section B de la 13ème chambre utilise pour sa part cette formulation : « *L'adresse IP ne permet pas d'identifier le ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur*. », v. : CA Paris, 27 avril 2007, 13e ch. Section B, RG n°06/02334, JurisData n°2007-338935.

personnel alors « que le simple constat probatoire de l'élément matériel d'une infraction commise sur l'internet par une individu utilisant un pseudonyme, dressé par l'agent assermenté d'un société de gestion collective, conformément à la législation sur la propriété intellectuelle, ne constitue pas un traitement de données personnelles, au sens du droit de l'informatique et des libertés, alors que seule la plainte auprès des autorités judiciaires, puis leurs investigations, ont conduit à l'identification de la personne, dans le cadre des règles de procédure pénale »[489]. Elle conclue en dissociant la procédure qui lui est soumise des traitements permettant une « surveillance automatisée des réseaux de peer-to-peer »[490].

Autrement dit alors qu'il n'y a pas d'identification automatique possible à partir de l'obtention de la seule adresse IP et qu'il n'y a pas de surveillance automatisée du réseau il est affirmé que le constat est valable en dehors de toute autorisation de la CNIL. Il faut souscrire à cette approche qui va être reprise par la plus haute juridiction française.

B] L'arrêt de la Cour de cassation du 13 janvier 2009

237. ***Plan.*** La Cour de cassation opère une pirouette en affirmant seulement qu'il n'y a pas en l'espèce de traitement automatisé **(1)**, un raisonnement qui est critiqué alors que cette affirmation aurait pu conduire à définir par ailleurs le caractère personnel de l'adresse IP **(2)**.

1) Le contenu de la décision : la pirouette de la Cour de cassation

238. **La pirouette de la Cour de cassation**. Par un arrêt du 13 mars 2009 la chambre criminelle de la Cour de cassation casse l'arrêt de la cour d'Appel de Rennes en date du 22 mai 2008 qui avait accueilli l'exception de nullité procédant du procès-verbal de constat de l'agent assermenté[491]. Cette décision de cassation au visa des articles 2, 9, 25 et 50 de la loi

---

[489] CA Paris, 15 mai 2007, 13e ch. section A, RG n°06/01954, JurisData n°2007-336454. La section B de la 13ème chambre utilise pour sa part cette formulation : « *Stéphane L. n'a pas recouru à un traitement de données personnelles qui aurait nécessité une autorisation préalable de la Cnil puisqu'il s'est contenté de se connecter à internet, d'accéder par un logiciel à des fichiers partagés et de recueillir l'adresse IP grâce au pseudonyme "thonio", ce que tout internaute pouvait faire ; dès lors, le prévenu n'ayant été identifié que dans le cadre d'une procédure judiciaire, la procédure est régulière*. ». CA Paris, 27 avril 2007, 13e ch. Section B, RG n°06/02334, JurisData n°2007-338935

V. également une décision ultérieure de la Cour d'appel de Paris dans le cadre non pas d'un contentieux visant un logiciel de P2P mais d'un site mettant à disposition des liens pour télécharger des œuvres ; le titulaire du nom de domaine et administrateur du site a été retrouvé grâce à l'adresse IP à l'origine des mises en ligne. La Cour énonce : « *le relevé de l'adresse IP de l'ordinateur ayant servi à l'infraction entre dans le constat de sa matérialité et pas dans l'identification de son auteur ; que cette série de chiffre ne constitue pas une donnée indirectement nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine et non à la personne qu'elle utilise ; que la consultation de sites accessibles au public ne permet que de déterminer que le fournisseur d'accès à internet mais aucunement l'utilisateur de l'ordinateur en cause ».* CA Paris, 28 mai 2008, 3ème ch. instr., RG 07/01064

[490] Ibid.

[491] Cass. crim., 13 janvier 2009, n°08-84088, *Bull. crim.* 2009, n°13, (JurisData n°2009-046824). V. sur cette décision : CARON Ch. « Validité des constats effectués par des agents assermentés »,*CCE.,* avril 2009, n°31, p.25 ; FLAMENT L., « Les constatations visuelles effectuées sur internet, sans recourir à un traitement préalable de surveillance automatisé ne constituent pas un traitement de données à caractère personnel (à propos de l'arrêt de la chambre criminelle du 13 janvier 2009) », *Dr. Pén.*,

Informatique et Libertés, et 226-19 et 226-23 du Code pénal n'apporte toutefois pas de réponse quant à la position du juge judiciaire suprême français sur la nature de l'adresse IP. En effet la Cour de cassation considère qu'il ne peut être conclu à la nullité du constat en cause en affirmant qu'il n'y a pas de traitement automatisé de données mais sans préciser si les données en question sont des données personnelles ou non[492].

Pour dénier l'existence de traitement la Cour de cassation énonce ainsi que l'agent assermenté au titre de sa mission effectue des « *constatations visuelles* » et recueille des renseignements en utilisant « *un appareillage informatique et un logiciel de pair à pair* » mais ce pour « *accéder manuellement* » aux données et que dès lors « *il se contente de relever l'adresse IP pour pouvoir localiser son fournisseur d'accès en vue de la découverte ultérieure de l'auteur des contrefaçons* ».

Un raisonnement qu'il faut saluer alors que l'utilisation d'un ordinateur et d'un logiciel pour accéder à une donnée numérique ne peut constituer un traitement automatisé. Il n'est pas non plus mis en œuvre ici un procédé informatique qui relève automatiquement les adresses IP se connectant aux réseaux P2P en vue d'une surveillance, automatique donc, et d'une répression qui pourrait être de grande ampleur ; le constat de l'infraction est le fait d'une personne physique l'agent assermenté[493]. Et la Cour de préciser que ce constat est bien le point de départ d'une investigation permettant d'identifier l'auteur de la contrefaçon. Il faut dès lors s'interroger sur la réserve de la chambre criminelle s'agissant de la qualification de l'adresse IP en tant que donnée à caractère personnel.

2) La critique de la position de la Cour de cassation

239. **La critique de la position de la Cour de cassation.** Alors que l'adresse IP peut être reliée à un FAI et à un point d'accès au réseau, elle permet de considérer la personne pouvant

---

mai 2009, études 10, p.11 ; ROBERT J.H., « Le travail manuel de l'informaticien », *Dr. Pén.,* mai 2009, comm. 66, p.30 ; TELLER M., « Les difficultés de l'identité numérique : quelle qualification juridique pour l'adresse IP ? », *D.*2009, n°29, chronique p.1988 ; DERIEUX E., « Lutte contre la contrefaçon et protection des données personnelles », *Légipresse,* n°261, mai 2009, p.98. V. également l'arrêt de la Cour d'appel de renvoi : CA Paris, pôle 5, ch. 12, 1er février 2010, (JurisData : 2010-000312).

[492] Le professeur Caron, soulignant le caractère «*un peu sibyllin* » de cet arrêt, énonce que : « Si l'on en croit la Cour de cassation, on a le sentiment que, au stade de sa collecte par l'agent assermenté, l'adresse IP ne semble pas répondre à la qualification de donnée personnelle », CARON Ch., *CCE, op. cit*. *Contra* : le professeur Jacques-Henri Robert affirme lui que « En statuant ainsi, la Cour de cassation admet implicitement que l'adresse IP est bien une donnée à caractère indirectement personnel, et elle se range à l'avis de la CNIL », ROBERT J.H, *Dr. Pén*., *op.cit*.

[493] Comme l'explique de manière très claire, le professeur Robert : « L'agent assermenté s'est assis devant un ordinateur qu'il a lui-même piloté pour repérer des échanges délictueux, au lieu d'employer un programme automatique apte à faire la besogne ; ensuite il n'a pas traité automatiquement les données recueillies, mais les a transmises matériellement aux officiers de police judiciaire en leur remettant des CD-ROM ou des images d'écran », ROBERT J.H, Droit pénal, *op.cit*.

être à l'origine de la connexion, présente au domicile de l'abonné par exemple, au moment de celle-ci.

Cités dans la décision du tribunal de Saint-Brieuc et abondamment repris dans les commentaires visant les décisions des juges du fond et l'arrêt de la Cour de cassation, les exemples du numéro de téléphone ou de la plaque d'immatriculation peuvent être repris[494]. Ces numéros sont attachés à une ligne téléphonique et à un véhicule et non à une personne : ils permettent de considérer les usages de ceux-ci et les personnes qui y ont accès. Ce sont des données à caractère personnel puisqu'elles sont relatives à un personne identifiée, l'abonné ou le titulaire de la carte grise et qu'elles permettent de retrouver par le biais d'une investigation l'auteur d'un appel ou le conducteur du véhicule. Elles sont relatives à une "*une personne identifiée*" et à "*une personne identifiable*" au sens de la loi Informatique et Libertés[495].

Toutefois on peut considérer la difficulté pour la Cour de cassation d'affirmer l'appartenance de l'adresse IP à la catégorie des données personnelles alors qu'il s'agit par nature d'une donnée numérique. Quand bien même l'arrêt fait un effort pour délimiter en l'espèce la notion de traitement automatisé, l'affirmation de la nature personnelle de l'adresse IP ne va-t-elle pas emporter la mise en œuvre de la loi Informatique et libertés pour toute collecte d'une telle adresse, produite automatiquement par toute connexion et visible ainsi par tout site web auquel un individu se connecte. On sent la difficulté de l'appréciation large du champ d'application de la loi Informatique et libertés qui ne vise plus des fichiers qui par leur seule mise en œuvre permettent l'identification automatique de l'individu, mais tout traitement automatisé de données en soi personnelles.

Mais, de fait alors que la catégorisation des deux notions, celle de « *donnée à caractère personnel* » et celle de « t*raitement automatisé* »ne sont plus liés ensemble par l'objectif visant l'encadrement de toute identification automatique de l'internaute, l'ensemble des juges européens puis par la suite la Cour de cassation, qui va clarifier sa position, vont affirmer que l'adresse IP est bien une donnée à caractère personnel.

[494] V. : LECLERCQ P., « Un an d'application de la loi Informatique et Libertés », *CCE*, octobre 2007, p.31 *;* SZUSKIN L., GUILLENCHMIDT (de) M., «La qualification de l'adresse IP au centre de la lutte contre le téléchargement illicite sur les réseaux peer-to-peer », *RLDI*, déc. 2007, n°1095 ; DROUARD E., BLANCHARD M., « L'adresse IP est-elle une donnée personnelle ? », *Légipresse*, n°255, octobre 2008, p.185

[495] V. : le communiqué de la CNIL en date du 2 Août 2007, « L'adresse est une donnée personnelle pour l'ensemble des CNIL européennes », disponible sur le site de la CNIL.

§2) L'affirmation désormais constante du caractère personnel de l'adresse IP

240. ***Plan.*** Par deux décisions en date du 19 octobre et du 3 novembre 2016, le juge européen et le juge suprême français mettent fin aux incertitudes qui pesaient sur la qualification de l'adresse IP en tant que donnée personnelle eu égard à son potentiel d'identification de l'internaute **(1)**. Une position qui laisse toutefois des questions en suspens puisque la donnée est jugée personnelle en soi en dehors de toute considération du traitement mis en œuvre pour la collecter et des conditions permettant l'identification de l'internaute **(2)**.

A] La position du juge européen et du juge suprême français

241. **L'impulsion de la CJUE.** En 2008, dans l'arrêt « *Promusicae* », la Cour de justice de l'Union Européenne est saisie d'une question préjudicielle qui porte sur la légalité de la demande d'une association de producteurs et d'éditeurs de musique espagnole qui souhaite obtenir communication auprès d'un FAI des coordonnées de l'abonné associés à une adresse IP visible sur un réseau P2P et ce dans le cadre d'une procédure civile[496]. La problématique est ici de considérer les conditions de ce rapprochement entre une adresse IP et les données personnelles réunies sous ce numéro par le FAI. Ce dernier peut-il communiquer les coordonnées de l'abonné dans le cadre d'une simple procédure civile, et non dans le seul cadre d'une procédure pénale[497] ?

Ainsi la formulation de l'arrêt et les conclusions de l'avocat général n'affirment pas la nature personnelle de l'adresse IP en tant que telle mais il est bien souligné qu'à cette donnée peuvent être associées des données à caractère personnel[498]. Autrement dit le juge européen est encore réticent à affirmer que l'adresse IP est une donnée personnelle, en ce que sa simple collecte ne permet pas d'identifier un individu[499], mais

---

[496] CJCE (*aff.* C-275/06), 29 janvier 2008, *Promusicae c/ Telefonica de Espana SAU*. V. notamment : LESUEUR J., « La balance sans l'épée : la droit fondamental sans l'effectivité », *Légipresse*,n°250, avril 2008, p. 57 ; CARON C. « La communication de données personnelles dans le cadre d'une procédure civile à l'aune du droit communautaire », *CCE*, mars 2008, commentaires n°32,p. 25.

[497] V. *infra* sur cette problématique : Titre II, chapitre 1er, Section II. « *La procédure permettant la divulgation du point d'accès utilisé* ».

[498] L'arrêt énonce que « Il n'est pas contesté que la communication sollicitée par Promusicae des noms et adresses de certains utilisateurs de KaZaA implique la mise à disposition de données à caractère personnel, c'est à dires des informations sur des personnes physiques identifiées ou identifiables conformément à la définition figurant à l'article 2 sous a) de la directive 95/46 », CJCE (aff. C-275/06), *op. cit*, point n°45.

L'avocate générale énonce pour sa part que « Communiquer à quels utilisateurs certaines adresses IP ont été attribuées à des moments précis implique la communication de données à caractère personnel au sens de l'article 2 sous a) de la directive 95/46 à savoir la divulgation d'informations sur des personnes physiques identifiées ou identifiables. Grâce à ces données, les opérations réalisées pourront être reliées au titulaire de la connexion en utilisant l'adresse IP correspondante », Conclusions de l'avocat général, Mme Juliane Kokott, présentées le 18 juillet 2007.

Logiquement ainsi il est affirmé que le FAI opère bien un traitement de données à caractère personnel en stockant au regard de toute adresse IP les coordonnées d'un de ses clients. Dans son ordonnance en 2009 dans le cadre de l'affaire *LSG c/ Tele2 Télécommunication Gmbh*, la Cour vise ainsi les « *données à caractère personnel relatives au trafic* » détenues par les opérateurs de communications électroniques.

[499] A l'inverse d'un numéro de téléphone fixe par exemple qui renvoie à un annuaire public.

elle est le point de départ d'un processus d'inférence qui permet de découvrir l'identité du titulaire de l'abonnement, et ce faisant après investigation, celle du contrefacteur. Dans son ordonnance en 2009 dans le cadre de l'affaire « *LSG c/ Tele2 Telecommunication Gmbh* », la Cour vise ainsi les « *données a caractère personnel relatives au trafic* » détenues par les opérateurs de communications électroniques[500].

En 2011 le juge européen dans l'affaire « *Scarlet c/ Sabam* » qui vise là encore un logiciel de P2P, clarifie sa position en énonçant qu'il est constant que ces adresses sont « *des données protégées à caractère personnel car elles permettent l'identification précise desdits utilisateurs* »[501]. Cette formulation ouvre la voie à une application large de la protection des données à caractère personnel s'agissant de toute collecte d'adresses IP puisqu'elle affirme la nature personnelle de l'adresse IP eu égard à son potentiel d'identification.

242. ***Plan.*** L'évolution de la jurisprudence fait ainsi apparaître que le raisonnement visant l'affirmation du caractère personnel de l'adresse IP va s'extraire du contexte de la lutte contre le téléchargement illégal. Dans l'arrêt *Breyer* la CJUE affirme qu'un site web allemand d'actualités ne peut conserver les adresses IP qui se connectent à lui sans le consentement des internautes que si le traitement poursuit une finalité légitime au sens de l'article 7 de la directive 95/46/CE **(a)** Dans l'arrêt de la Cour de cassation il est affirmé qu'un site web interne d'annonces immobilières ne peut collecter les adresses IP qui se connectent à lui s'il n'en a pas informé la CNIL en application de l'article 22 de la loi Informatique et Libertés. **(b)**.

1) L'arrêt « Breyer » de la CJUE du 19 octobre 2016.

243. **L'adresse IP est objectivement une donnée personnelle.** En 2016 l'affaire *Breyer* donne la possibilité à la CJUE de confirmer cette appréciation large du caractère personnel de l'adresse IP alors que les faits du contentieux ne visent plus les conditions d'accès au fichier mis en œuvre par le FAI mais l'enregistrement de l'adresse IP d'un particulier par un site web[502].

Le juge du fond allemand a conclu qu'un tel enregistrement était valable alors que l'adresse IP pour l'exploitant du site n'est pas une donnée personnelle[503]. La Cour

[500] CJCE, ordonnance (8ème ch aff. C-557/07), 19 février 2009, *LSG c/ Tele2 Télécommunication Gmbh.*

[501] CJUE (aff. C-70-10), 25 novembre 2011, *Scarlet Extended SA c/SABAM et al*, point n°51. V. : *D.* 2011, 2925, obs. C.MANARA

[502] CJUE (aff. C-583/14), 19 octobre 2016, *Patrick Breyer c/ Bundesrepublik Deutschland*. V. : PERONNE G., DAOUD E., « L'adresse IP est bien une donnée à caractère personnel », *D. IP/IT*, 120, février 2017.

[503] *Ibid.*,point n°21.

fédérale de justice allemande (le *Bundesgerichtstof)* est partagée ne sachant pas s'il convient pour la qualification de cette donnée, de se fonder sur un critère « objectif » ou « relatif »[504]. Dans le premier cas l'adresse est personnelle en elle-même et tous ceux qui la détiennent quand bien même ils ne détiennent pas les éléments la rattachant à une personne identifiée ou identifiable opèrent un traitement de données personnelles ; dans le second cas l'adresse n'est une donnée personnelle que pour le FAI qui met en œuvre le fichier l'associant à la localisation physique de la machine utilisée. Une question préjudicielle est posée à la CJUE ; elle va alors affirmer que l'adresse de protocole internet dynamique d'un visiteur constitue bien, pour l'exploitant du site, une donnée à caractère personnel, lorsque cet exploitant dispose de moyens légaux lui permettant de faire identifier le visiteur concerné grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet du visiteur[505].

244. **Le critère de la nature des moyens raisonnables à mettre en œuvre pour identifier un individu**. Pour fonder ce choix du critère objectif, il est d'abord énoncé que : « *L'utilisation par le législateur de l'Union du terme « indirectement » tend à indiquer que, afin de qualifier une information de donnée à caractère personnel, il n'est pas nécessaire que cette information permette, à elle seule, d'identifier la personne concernée* »[506]. Ainsi la logique originelle de la mise en œuvre d'un fichier de données est prise en compte. En effet l'identification est directe si un fichier de données est établi au nom d'un individu et indirecte si à ce nom est substitué un numéro. Ainsi il convient dès lors de comprendre que le numéro IP est une donnée personnelle par le truchement du fichier qui le rattache aux coordonnées d'un abonné mis en œuvre par le FAI. Et la Cour précise qu' *« il n'est pas requis que toutes les informations permettant d'identifier la personne concernée doivent se trouver entre les mains d'un seule personne* »[507].

Le critère permettant alors de considérer si la donnée que détient la personne est personnelle ou non est celui de la nature des moyens qu'elle doit mettre en œuvre pour identifier la personne concernée ; si ces moyens sont raisonnables, la donnée en sa possession est personnelle[508]. En l'espèce la Cour conclue qu'alors que des voies légales permettent à l'exploitant du site de requérir les données à disposition du FAI notamment

[504] *Ibid.*,point n°25.
[505] *Ibid.*,point n°49.
[506] CJUE (aff. C-583/14), 19 octobre 2016, *Patrick Breyer c/ Bundesrepublik Deutschland*, point n°41.
[507] *Ibid.*, point n°43.
[508] *Ibib.*, points 45 à 47. La CJUE rappelle le considérant 26 de la directive 95/46 et les conclusions de l'avocat général au point 68 : « *tel ne serait pas le cas si l'identification de la personne concernée était interdite par la loi ou irréalisable en pratique, par exemple en raison du fait qu'elle impliquerait un effort démesuré en termes de temps, de coût et de main-d'œuvre, de sorte que le risque d'une identification paraît en réalité insignifiant ».*

pour la mise en œuvre de poursuites pénales, l'exploitant du site dispose ainsi de ces moyens raisonnables d'identification[509].

2) L'arrêt « Logisneuf » de la Cour de cassation du 3 novembre 2016

245. **La reconnaissance du caractère personnel de l'adresse IP.** Dans cet arrêt[510], les administrateurs d'un réseau interne d'entreprise, celui d'un groupe immobilier, constatent que des adresses IP n'étant pas attribuées aux machines du réseau se connectent pourtant à celui-ci et utilisent les codes d'accès nécessaires pour consulter le contenu des informations mises à disposition sur celui-ci. Pour être clair, si l'on fait un parallèle avec le monde réel, l'extranéité des adresses IP montre que des tiers non habilités se sont introduits dans le réseau informatique du groupe immobilier pour consulter ses annonces immobilières exclusives. Les sociétés du groupe immobilier saisissent alors le juge des requêtes pour obtenir communication des coordonnées des abonnés associés à ces adresses IP auprès des FAI. Le juge fait droit à leur demande et il apparaît que ces adresses ont été attribuées aux connexions d'une société de gestion de patrimoine concurrente à celles des demandeurs.

Cette société concurrente mise en cause invoque l'illicéité de la mesure d'instruction sollicitée ; selon elle, la conservation, sous forme de fichier, de ces adresses IP, aurait du faire l'objet d'une déclaration auprès de la CNIL. Toutefois dans un arrêt du 28 avril 2015 le président du tribunal de Grande Instance rejette la demande de rétraction de l'ordonnance rendue sur requête. Il énonce que l'adresse IP « *se rapporte à un ordinateur et non à l'utilisateur, et ne constitue pas dès lors une donnée même indirectement nominative* »[511]. Il poursuit en affirmant que « *La loi en question vise en outre les personnes physiques, identifiées directement ou indirectement. Les adresses IP peuvent être attribuées à des personnes morales et la conservation de ces données ne relève alors en tout état de cause pas de ces dispositions légales. Le fait de conserver, en vue de la découverte ultérieure des auteurs de pénétrations non autorisées […] sur un réseau informatique d'entreprise, sans qu'aucun lien entre ces adresses et des personnes ne soit fait, ne constitue pas un traitement de données à caractère personnel* »[512].

Le caractère pervers du contentieux des logiciels de P2P apparaît à nouveau ; en réalité la problématique est celle de la surveillance de l'accès à un site et des conditions

[509] *Ibid.*, point n°47.

[510] Cass., civ. 1ère.,3 nov. 2016, 15-22595, FS+P+B+I Cabinet Peterson c/ groupe Logisneuf et autres. V. : PERONNE G., DAOUD E., « L'adresse IP est bien une donnée à caractère personnel », *D. IP/IT*, 120, février 2017 :

[511] CA Rennes, arrêt rendu le 28 avril 2015.

[512] *Ibid.*

de divulgation des coordonnées d'un abonné, et non celle de la qualification de l'adresse IP en tant que donnée à caractère personnel. L'objectif du président du TGI est moins tant de contester ce caractère personnel de l'adresse IP que de permettre à l'exploitant d'un site de connaître qui est à l'origine d'une connexion illégale à celui-ci et d'engager une action non pas contre un individu identifié mais en l'espèce ici une société commerciale.

Or le juge suprême français ne peut opérer ce raisonnement alors que le champ d'application de la loi Informatique et Libertés qui s'entend de manière objective ne peut que mener à l'inclusion de l'adresse IP dans celui-ci. En effet d'une part, cette appréciation large fait désormais consensus et a été reconnue par la CJUE quelques semaines auparavant. D'autre part les faits de l'espèce, à la différence de ceux de 2009, ne font pas apparaître le simple relevé d'une adresse IP visible sur le réseau. Pour constater une intrusion, il a fallu mettre en place des procédés détectant les connexions des adresses IP étrangères au réseau et conserver sous forme de fichiers journaux ces données relatives à ce que l'on peut appeler des attaques. La Cour de cassation affirme ainsi que « *Les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte doit faire l'objet d'une déclaration préalable* »[513].

Ainsi toute collecte d'adresses IP visibles sur le réseau doit faire l'objet d'une formalité préalable auprès de la CNIL ce qui pose question alors qu'il est nécessaire pour tout site de pouvoir ménager une possibilité d'identification de ses utilisateurs.

B] Les questions en suspens eu égard à la portée de ces arrêts

246. ***Plan***. La portée des arrêts « *Breyer* » et « *Logisneuf* » interroge alors que leur raisonnement invite à mettre en œuvre une balance des intérêts qui se cantonne nécessairement aux faits de l'espèce **(a).** Il faut affirmer l'inadéquation du champ d'application de la protection des données personnelles à l'adresse IP qui ne peut être considérée comme une donnée personnelle en soi **(b).**

1) La difficile mise en balance des intérêts en présence.

247. La portée de l'arrêt *Breyer* : la nécessaire mise en balance des intérêts en présence présidant à la création d'un fichier d'adresses IP des visiteurs par un site web. La première partie du raisonnement du juge européen en application de la directive 95/46 n'est pas critiquable : elle consacre la qualification par l'instance juridictionnelle européenne de

[513] Cass., civ. 1ère., 3 nov. 2016, 15-22595, *op. cit.*

l'adresse IP en tant que donnée à caractère personnel. C'est la seconde qui en découle automatiquement qui l'est. Elle démontre la limite de l'application de la directive qui ne précise pas les modalités de mise en œuvre des fichiers de telles données.

Le juge européen condamne en effet la législation allemande qui ne permet l'enregistrement de l'adresse IP en l'absence du consentement de l'internaute qu'à des fins de facturation du service. Cette législation est trop restrictive et ne permet pas d'opérer une balance des intérêts entre les droits et libertés fondamentaux de la personne concernée et la libre-circulation des données et dès lors l'intérêt du responsable du traitement. Les adresses IP doivent pouvoir être conservées en application de l'article 7 f) de la directive pour permettre la réalisation de l'intérêt légitime de celui-ci[514]. La CJUE énonce ainsi que les sites visés qui fournissent des services de médias en ligne pourraient avoir un intérêt légitime « *à garantir, au-delà de chaque utilisation concrète de leurs sites Internet accessibles au public, la continuité du fonctionnement desdits sites »*[515]. Toutefois le juge conclut en l'espèce que le seul objectif du site web «*visant à garantir la capacité générale de fonctionnement »* de son service ne peut être considéré comme une finalité légitime pouvant justifier une atteinte au droit à la protection des données des visiteurs[516].

On comprend ainsi que la finalité de la collecte visée en l'espèce est trop large et diffère d'un objectif visant la continuité du service, autrement dit la détection d'attaques informatiques. De fait si des voies légales ont été aménagées pour permettre la mise en cause d'internautes identifiés par les sites notamment en cas d'attaques cybernétiques, il faut pourvoir conserver des adresses IP des visiteurs du site sans leur consentement.

Cependant des questions restent en suspens sur la mise en œuvre d'une telle balance d'intérêts. Ne peut-on pas considérer que tout site web puisse conserver une trace d'une connexion à ses services ? La dématérialisation des services sur le web n'entraîne-t-elle pas une nécessité de ménager une possibilité d'interaction physique avec l'internaute par le biais de la mémorisation de son adresse IP ? Or si l'on répond par la positive en considérant ici une finalité légitime qui permet de ne pas recueillir le consentement de l'internaute, il faut toutefois souligner que la législation française rend alors nécessaire qu'un tel fichier soit déclaré. Cette application des formalités préalables montre les limites d'un encadrement de la collecte des adresses IP en application des principes généraux de la protection des données personnelles.

[514] *Ibid.,* points n°55 à 58.
[515] *Ibid.,* point n°60.
[516] *Ibid.,* point n°64, en application de l'article 7, sous f) de la directive 95/46.

248. **La portée de l'arrêt de la Cour de cassation : le sens d'une telle déclaration préalable auprès de la CNIL**. Il faut affirmer ainsi que cette reconnaissance jurisprudentielle qui lève désormais tout doute sur le caractère personnel d'une adresse IP[517] ne résout pas la problématique du champ d'application de la loi Informatique et Libertés. En effet cela implique donc que toute collecte d'adresses IP soit soumise à une déclaration préalable sur le fondement de l'article 22 de la loi de 1978. Tout administrateur de site doit ainsi considérer que s'il n'en a pas informé la CNIL, il ne peut enregistrer dans un fichier une adresse IP qui s'est connectée aux serveurs et sites dont il a la gestion.

Clémence Scottiez, chef du service économiques de la CNIL, évoquait dans une conférence organisée conjointement par le master 2 Droit du Multimédia et de l'Informatique et le CEJEM de l'université Paris 2 en mars 2017[518], les conséquences d'une telle exigence qui nécessairement renvoie à une multiplication des déclarations et même à une nouvelle problématique s'agissant de savoir si une autorisation est nécessaire alors que bien souvent les adresses sont relevées pour constater une infraction. Elle expose ainsi l'exemple d'un site de rencontre qui souhaitait enregistrer les adresses IP utilisées par certains de ses utilisateurs et ce afin de détecter les faux profils. Elle cite une décision du tribunal d'instance de Nancy qui a reçu comme preuve valable le relevé des adresses utilisées pour la création des comptes utilisateurs[519]. Or Mme Scottiez s'interroge : la mise en œuvre d'un faux-profil constitue-t-elle une infraction ? Même en cas de réponse négative, la sanction prise par le site de bannir l'utilisateur ne renvoie-t-elle pas à un traitement visant l'exclusion d'un individu, traitement qui lui aussi doit être autorisé par la CNIL ? Elle soulignait que l'objectif actuel était alors de rationnaliser ces problématiques avec des normes. De fait le nouveau règlement européen visant la protection des données à caractère personnel supprime toute exigence de formalités préalables mais il convient néanmoins de

[517] DEBET A., MASSOT J., METALLINOS N., Informatique et Libertés, la protection des données personnelles en droit français et européen, L.G.D.J.,Paris, 2015, n° 210 et 523.

[518] « L'adresse IP : une empreinte digitale sur internet ? », conférence organisée par le Master 2 Droit du multimédia et de l'Informatique et le CEJEM (Centre d'études juridiques et économiques du multimédia) de l'université Paris 2, jeudi 2 mars 2017. L'intervention de Mme Scottiez avait pour intitulé « L'adresse IP, une donnée à caractère personnel ? ».

[519] La mise en œuvre de deux profils à partir d'une même adresse IP et la connexion à ceux-ci à partir d'une même adresse dans un laps de temps court fait apparaître qu'une même personne les a créés et les utilise.

V. sur ce point : le jugement du tribunal d'instance de Nancy en date du 5 septembre 2014, M.C./ Société Netuneed, disponible en ligne sur le site légalis.fr. Le relevé des adresses IP à l'origine de la création et de la consultation de 13 comptes membres du site OVS est reçu comme preuve de la création de faux-profils. Alors que l'internaute a manqué aux conditions générales d'utilisation du site, il est affirmé que son bannissement prévu dans ces mêmes conditions est la conséquence logique de ses actes et que l'internaute ne saurait prétendre à aucun dommage et intérêts de ce fait sur le fondement de l'article 1147 du code civil.

respecter les conditions de licéité du traitement. Ainsi s'il n'apparaît pas que le traitement a une finalité légitime, le consentement de l'internaute est requis.

Or à titre d'exemple il peut être ici fait mention du fichier d'adresses IP à disposition de toute personne disposant d'un compte de messagerie *gmail*. En effet la société *Google* met à disposition du titulaire de la messagerie un outil lui permettant de voir l'ensemble des adresses IP qui se sont connectées à sa boîte mail[520]. Celui-ci peut alors distinguer celle qui n'est pas la sienne. En effet, ces adresses ne doivent être que celles des points d'accès auxquels s'est connecté le titulaire du compte (adresse du wifi de son domicile, adresse du wifi de son lieu de travail, adresse de l'abonnement 3G de son Smartphone, etc.). La consultation du tableau de ces adresses IP et de leurs dates et heures de connexion peut ainsi révéler, si elles ne correspondent pas aux usages de l'utilisateur, une intrusion dans la boîte mail. On le voit, la mise en œuvre de tels fichiers est généralisée puisqu'elle répond d'une nécessité de sauvegarder l'intégrité des systèmes informatiques et à un objectif légitime de surveillance des connexions au réseau.

La réelle problématique est celle de la mise en œuvre de cette surveillance. L'enjeu est-il celui du droit de la personne à la protection de ses données personnelles ? La réponse est non.

2) L'inadéquation du champ d'application de la protection des données personnelles.

249. **Aucune donnée n'est personnelle en soi**. La limite de l'élargissement du champ d'application de la loi Informatique et Libertés est qu'il invite à se questionner sur le potentiel d'identification d'une donnée et à dissocier dès lors la nature de la donnée des fonctionnalités du traitement qui la met en œuvre. La problématique est alors de savoir si la donnée est personnelle en soi. Or aucune donnée ne l'est.

Ainsi on ne peut affirmer que l'adresse IP est une donnée personnelle de la même manière que l'on ne peut soutenir qu'elle n'est pas une donnée personnelle puisque l'identification qu'elle permet est fonction des circonstances dans lesquelles il peut être accédé au fichier de l'opérateur de communications électroniques. Ce que l'on peut affirmer en revanche c'est que l'adresse IP en soi ne permet pas d'identification automatique d'un individu. Elle n'est un identifiant, c'est-à-dire le numéro univoque

[520] Pour accéder à cet outil, ouvrir votre compte de messagerie *Gmail*, visualisez en haut à droite le symbole d'une roue dite « paramètres », cliquez sur ce symbole, dans le menu déroulant, cliquez sur « paramètres », déroulez la page s'affichant jusqu'en bas ; il est indiqué à droite, les minutes écoulées depuis la dernière utilisation du compte, cliquez sur le terme « détails » affiché juste en dessous de cette mention.

attribué à un individu, que dans le cadre du fichier mis en œuvre par l'opérateur de communications électroniques et s'agissant uniquement d'un abonné. Or un auteur montre bien les spécificités de ce fichier[521]. D'une part doit être prise en compte la répartition dynamique des adresses IP ; qui implique que la seule adresse ne peut mener à l'abonné si elle n'est pas complétée par la date et l'heure de connexion. D'autre part, à la différence de l'annuaire téléphonique, ce fichier n'est pas à disposition de tous.

Il n'est donc pas non plus d'identification indirecte permise dans l'absolu par ce numéro. Les propos des professeurs Gautier et Caron tenus dans leurs manuels de propriété littéraire et artistique respectifs peuvent être repris sans qu'il faille revenir sur le contexte de la lutte contre le téléchargement illégal et la condamnation nécessaire de tout acte de contrefaçon sur le réseau. Ainsi le professeur Gautier soutient que les agents assermentés « *peuvent instrumenter sur l'internet et relever l'adresse IP des contrefacteurs, qui en soi, n'est pas une donnée personnelle, fût-elle indirecte, l'identification de ceux-ci étant assurée dans un deuxième temps, soit par les autorités de police ou de gendarmerie interrogeant le FAI, soit par les agents de la HADOPI, soit par les autorités de gestion collective elles-mêmes si elles en ont reçu l'autorisation de la CNIL dans le cadre des articles 2, 9 et 25 de la loi du 6 janvier 1978 modifiée*»[522]. De la même manière le professeur Caron souligne qu' «*il est possible d'en déduire qu'au moment de sa collecte, elle ne peut être qualifiée de donnée à caractère personnel même si, par la suite, elle est susceptible de le devenir* »[523].

Une procédure aux conditions strictes nécessitant l'intervention d'une autorité compétente est définie pour faire coïncider un numéro IP avec les coordonnées d'un abonné.

250. **L'enjeu de la protection de la liberté individuelle**. Il faut ainsi souligner qu'il n'est énoncé dans aucun texte que « L'adresse IP est une donnée à caractère personnel ».

En 2009, les sénateurs Detraigne et Escoffier présentent une proposition de loi « *visant à garantir le droit à la vie privée à l'heure du numérique* » qui souhaite « *affirmer sans ambiguïté que l'adresse IP constitue une donnée à caractère*

[521] « Ensuite la simple connaissance d'une adresse IP ne peut permettre l'identification directe d'une personne. Si le détenteur d'un numéro de téléphone peut se servir d'un annuaire inversé-gratuitement disponible sur internet- pour identifier son correspondant, la possession d'une adresse IP impose une demande d'autorité compétente auprès d'un opérateur internet », FLAMENT L., « Le numéro IP n'est pas une donnée à caractère personnel-La cour d'appel de Paris persiste et signe ! », Droit Pénal, n°12, décembre 2008, étude 27.

[522] GAUTIER P.-Y., *Propriété littéraire et artistique*, 7ème éd., P.U.F (Coll. Droit fondamental classique) : Paris, 2010, n°737.

[523] CARON Ch., *Droit d'auteur et droits voisins*, 2ème éd., LexisNexis Litec (Manuel) : Paris, 2009, n°540.

personnel. »[524]. Il est proposé de modifier l'article 2 de la loi Informatique et libertés pour préciser que « constitue en particulier une donnée à caractère personnel toute adresse ou tout numéro identifiant l'équipement terminal de connexion à un réseau de communication »[525]. Cependant des personnes auditionnées dans le cadre de cette étude ont fait part de leurs réserves quant à trancher en ce sens sur le statut de l'adresse IP. Cette proposition de loi n'a finalement pas été adoptée définitivement par le Parlement. Le Conseil d'État dans son rapport de 2014, intitulé « Le numérique et les droits fondamentaux », le regrette et énonce que « L'adresse IP doit donc être considérée comme une donnée à caractère personnel »[526]. Une affirmation qui n'est pourtant pas reprise dans la loi pour une République numérique. Elle ne l'est pas non plus dans le nouveau règlement européen sur la protection des données.

En effet, en 2016 le nouveau règlement européen relatif à la protection des données à caractère personnel et à la libre-circulation de celles-ci adopte une nouvelle définition de la donnée à caractère personnel dans la droite ligne de celle de 1995 qui visait une application large de la règlementation. Il est ainsi énoncé qu'une donnée à caractère personnel est « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ; »*[527]. La notion d' « *identifiant* » et la mention du « *numéro d'identification* » font référence à l'adresse IP. Toutefois sa nature personnelle n'est pas affirmée en soi et ne peut l'être.

Dans sa proposition de règlement, la Commission européenne indiquait ainsi que : « *Il en découle que des numéros d'identification, des données de localisation, des identifiants en ligne ou d'autres éléments spécifiques ne doivent pas nécessairement être considérés, en soi, comme des données à caractère personnel dans tous les cas de*

[524] Recommandation n°10 du rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques de M. Yves Detraigne et Mme. Anne-Marie Escoffier, n°441, Sénat, (session ordinaire de 2008-2009), p. 98.

[525] Article 2 de la proposition de loi « visant à mieux garantir le droit à la vie privée à l'heure du numérique », présentée par M. Yves Detraigne et Mme. Anne-Marie Escoffier, n°93, Sénat, , (session ordinaire de 2009-2010).

[526] Conseil d'État, « Le numérique et les droits fondamentaux », étude annuelle 2014, p. 171.

[527] Article 4 « Définitions », 1) du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre-circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JORF L119/1-88.

figure »[528]. Ils ne le sont que eu égard à des circonstances de collecte et à une procédure d'accès aux données d'identification de la personne. L'enjeu ici, n'est pas celui de la protection d'une donnée personnelle mais celui de la protection de la liberté individuelle qui impose qu'un individu ne puisse être identifié que dans des conditions strictes et ne fasse pas l'objet d'une surveillance arbitraire.

[528] Considérant 24, Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre-circulation de ces données (règlement général sur la protection des données), 2012/0011 (COD).

Conclusion du chapitre 1er

251. **Le lien entre une adresse IP et un individu identifié et identifiable**. Il a été montré que l'adresse IP est le pendant du numéro de téléphone sur le réseau internet. Elle permet, non pas la mise en œuvre d'un appel téléphonique, mais une connexion au réseau. Elle renvoie dès lors aux coordonnées de l'abonné et à un champ d'investigation géographiquement restreint s'agissant de l'internaute connecté.

En effet les adresses IP sont réparties publiquement à l'échelle mondiale entre tous les opérateurs de communications nationaux. La fonction de ces opérateurs est de permettre un accès au réseau ; c'est-à-dire qu'ils doivent tout aussi bien mettre à disposition un point d'accès à la structure du réseau mondial mais également organiser l'adressage des connexions mises en œuvre à partir de ce point. Or la mise à disposition d'un point d'accès à la structure est l'objet du contrat d'abonnement et l'adressage des connexions répond d'une logique technique qui délimite un périmètre de connexion.

Ainsi d'une part un opérateur est en lien avec un abonné identifié puisqu'il monnaie son service. Cet abonné peut être un particulier, comme dans le cas des services offerts par un FAI, mais également une personne morale, comme une université ou une collectivité locale ou une entreprise. L'opérateur attribue une adresse IP fixe ou dynamique à la « box » du particulier ou au serveur de la collectivité. Dans le second cas, l'adresse n'est attribuée que le temps de la connexion et peut servir à mettre en œuvre, à un autre moment, la connexion d'un point d'accès faisant l'objet d'un autre abonnement. Pour considérer l'abonnement utilisé, la date et l'heure attachée à l'adresse IP deviennent alors un critère discriminant.

Il peut être ainsi affirmé que l'opérateur de communications électroniques peut relier une adresse IP aux coordonnées d'un abonné, personne physique ou morale. Dans le cadre de la prestation mise en œuvre par un FAI l'adresse IP peut être reliée à un individu identifié, le particulier abonné.

D'autre part un point d'accès au réseau ne peut faire l'objet d'un nombre de connexions illimité et recouvre nécessairement un périmètre de connexion restreint. Ainsi dès lors qu'un accès ne fait pas l'objet d'un usage domestique qui se limite à la connexion au même moment de quelques machines à partir du point d'accès au réseau mondial, un sous-réseau local doit être créé et faire l'objet d'un adressage propre dit « privé ». Une concordance s'établit entre l'adresse IP publique visible sur le réseau

mondial et une adresse IP privée qui renvoie à un nouveau nœud de connexion. Ce nœud délimite un espace géographique restreint de connexion, une prise filaire ou un signal wifi d'une portée de quelques mètres, dans la même logique exactement que celui du réseau domestique.

Dès lors l'adresse IP peut être reliée à un individu identifiable, l'internaute connecté au réseau grâce à la mise en œuvre d'une investigation efficace qui n'a à considérer qu'un espace restreint de connexion.

252. **La reconnaissance jurisprudentielle du caractère personnel de l'adresse IP**. Il a ainsi été rappelé qu'à l'origine un consensus existe sur la nature personnelle de l'adresse IP puisqu'elle est attribuée par un opérateur à un abonné dans le cadre d'une connexion au réseau et qu'elle permet dès lors de considérer son point d'accès et les personnes qui s'y sont connectées.

La problématique du champ d'application de la protection des données personnelles apparaît dans le cadre du contentieux visant la lutte contre le téléchargement illégal et la surveillance des réseaux P2P que souhaite mettre en œuvre les sociétés de droits d'auteurs. Alors que les mécanismes de la HADOPI ne sont pas encore adoptés, l'application de la loi Informatique et Libertés à la collecte des adresses IP visibles sur de tels réseaux permet de circonscrire cette surveillance en veillant à ce qu'elle ne soit pas automatique. Si des crispations jurisprudentielles ont pu avoir lieu quant à la qualification des traitements ou relevés de telles adresses mis en œuvre par les sociétés de droit d'auteur et leurs agents assermentés, l'élargissement du contentieux qui vise désormais la collecte d'une adresse IP par tout site web permet aux juges suprêmes européen et français d'aboutir à un raisonnement constant.

Deux arrêts en 2016 viennent lever tout doute sur le caractère personnel de l'adresse IP[529]. L'adresse IP est une donnée à caractère personnel puisque des procédures légales ont été définies pour permettre un accès aux données détenues par l'opérateur de communications électroniques. En effet, il faut pouvoir identifier les auteurs d'infractions, et les sites web peuvent légitimement mettre en œuvre une collecte des adresses IP qui se connectent à leurs services sans le consentement des internautes dès lors qu'une telle collecte vise cette finalité précise, notamment en ce qui concerne la détection des auteurs d'attaques informatiques. Autrement dit le site web a des moyens

[529] CJUE (aff. C-583/14), 19 octobre 2016, *Patrick Breyer c/ Bundesrepublik Deutschland* ; Cass., civ. 1ère.,3 nov. 2016, 15-22595, Cabinet Peterson c/ groupe Logisneuf et autres.

raisonnables d'identifier l'internaute connecté s'il met en œuvre le traitement à des fins de poursuites.

On sent ici la limite du champ d'application de la protection des données personnelles alors que l'objectif n'est plus celui de prévenir le risque d'identification automatique de l'individu mais de considérer dans quelle mesure peut être mis en œuvre un contrôle d'identité. Le raisonnement devient nécessairement spécieux, en ce sens qu'il doit viser à chaque fois les circonstances de l'espèce et opérer une mise en balance des intérêts en présence pour en réalité répondre à une question d'ordre public : dans quelle mesure doit-on pouvoir identifier un internaute qui s'est connecté à un site web ?

253. **L'inadéquation du champ d'application de la protection des données à caractère personnel**. Il doit être soutenu qu'aucune donnée n'est personnelle en soi. Le potentiel d'identification d'une donnée doit se mesurer à l'aune d'un traitement et ce qu'il convient de prohiber est l'identification automatique d'un individu à partir des données produites par sa seule connexion au réseau.

Il faut critiquer ici l'objectivisation du champ d'application de la protection des données personnelles qui fait de l'objet à protéger, les données personnelles introduites dans un fichier, l'objectif de la protection. Il ne faut plus encadrer les traitements qui identifient automatiquement un individu mais se prémunir du risque d'identification ; ainsi la donnée est personnelle dès lors qu'elle peut conduire à l'identification d'un individu. On comprend cet enjeu à l'heure du développement de la technologie numérique qui numérise donc toute donnée et permet l'interconnexion de celles-ci, ce qui multiplie les possibilités qu'un individu soit identifié à partir de ces seules données, c'est-à-dire en dehors de toute investigation, à partir d'un procédé entièrement automatisé.

Toutefois ce mécanisme ne peut être généralisé et viser toute donnée numérique. De fait les juges ont reconnu le caractère personnel de l'adresse IP en considération du traitement, pour chaque cas d'espèce, qui la met en œuvre. Aucun texte législatif n'est venu et ne viendra affirmer que l'adresse IP est une donnée à caractère personnel. S'il fut un temps envisagé une telle éventualité dans le cadre du règlement européen, elle n'a pas abouti et pour cause[530].

[530] V. le considérant n° 24 de la « Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre-circulation de ces données (règlement général sur la protection des données), » 2012/0011 (COD), et l'article 4 « Définitions », 1) du « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre-circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JORF L119/1-88.

En effet si l'adresse IP est par essence une donnée numérique, elle ne permet pas l'identification automatique d'un individu. Elle ne permet le rapport à un abonné que dans le cadre de l'accès au fichier de l'opérateur de communications électroniques. L'accès aux données de ce fichier est strictement encadré par la loi. Il ne s'agit évidemment pas d'un fichier public qui opèrerait le rapprochement entre un numéro IP et un abonné à l'instar de l'annuaire téléphonique. L'adresse IP ne permet pas d'identifier indirectement et automatiquement un abonné par quiconque la détient ; elle ne le permet que dans le cadre d'une procédure légalement définie qui délimite les contours du contrôle de l'identité de l'internaute.

254. **L'analogie à mettre en œuvre : l'adresse IP doit être considérée comme le visage découvert de l'internaute.** Ainsi la solution proposée pour envisager les enjeux d'une donnée telle que l'adresse IP est de considérer celle-ci comme le visage découvert d'un internaute. La même problématique qui fut celle de la vidéosurveillance en son temps apparaît alors que la CNIL à l'époque critiquait que de tels procédés soient soustraits à son contrôle arguant de la nature personnelle du visage d'un individu[531].

En réalité les traits d'un visage ne renseignent dans l'absolu sur aucune identité et l'on doit s'en garder. Le développement de la « reconnaissance faciale » inquiète aujourd'hui et il convient d'encadrer ce procédé alors qu'un individu ne peut être identifié à son insu automatiquement par le relevé des seuls traits de son visage[532].

Il convient de considérer que les mêmes enjeux apparaissent aujourd'hui sur le réseau s'agissant de la mise en œuvre de l'adressage et de la collecte des adresses IP. Il faut ménager la possibilité qu'une adresse IP puisse mener à l'identification d'un internaute connecté sans que celle-ci puisse se faire automatiquement, et il faut définir les conditions de ce contrôle d'identité qui ne peut ressortir que du pouvoir régalien.

[531] CNIL, Délibération 94-056 du 21 juin 1994 **« portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et les lieux recevant le public ».**

[532] LEPLÂTRE Simon, « En Chine, la reconnaissance faciale envahit le quotidien », *Le Monde*, lundi 11 décembre 2017.

Chapitre 2ème. L'encadrement de l'identification de l'internaute à partir de son adresse IP

255. **Le rôle de l'adresse IP dans l'identification de l'internaute connecté**. Dans l'ouvrage « *Informatique et Libertés, la protection des données à caractère personnel en droit français et européen* », de A. Debet, J. Massot et N. Mettalinos, il est écrit que « *L'adresse IP appelle une attention particulière en ce sens qu'elle est, contrairement aux autres données de connexion, systématiquement collectée lors de chaque connexion au réseau et qu'elle peut être reliée, au moins par le fournisseur d'accès Internet si elle est combinée avec la date de connexion, à chaque compte utilisateur »*[533]. Il faut dans cette assertion dissocier deux idées : d'une part l'adresse IP est une donnée produite automatiquement par toute connexion au réseau, d'autre part l'adresse IP peut être reliée à un abonné identifié grâce au fichier mis en œuvre par le FAI.

Or il faut tout d'abord à nouveau affirmer que si l'adresse IP est produite automatiquement par toute connexion au réseau elle ne permet pas l'identification automatique de l'internaute. Son automatisme n'a pas à appeler d'attention particulière alors qu'étant l'identifiant d'une connexion et non d'un individu cette donnée ne permet ni une identification directe, ni indirecte de l'internaute connecté pour toute personne qui la visualise. Il faut respecter cette logique. Il faut considérer que ne peut se superposer au mécanisme d'adressage du réseau un système d'identification de l'internaute dont la liberté d'accès serait méconnue s'il avait à s'identifier préalablement à toute connexion au réseau.

Cela établi, la seconde partie du raisonnement intervient : les adresses IP collectées ne peuvent mener à l'identification de l'internaute que dans le cadre de l'accès aux données conservées par les acteurs de l'adressage du réseau. Or c'est ce fichier qui renvoie à une attention particulière. En effet c'est la conservation de telles données qui permet le contrôle de l'identité de l'internaute. Or l'adressage est une action qui répond d'une logique d'immédiateté et d'impermanence. Ainsi à cet endroit un régime légal doit intervenir qui organise le fichage des points d'accès au réseau au regard des connexions opérées pour qu'une investigation efficace puisse avoir lieu.

[533] DEBET A., MASSOT J., METALLINOS N., Informatique et Libertés, la protection des données personnelles en droit français et européen, L.G.D.J.,Paris, 2015, n° 518.

256. ***Plan.*** Il convient ainsi dans un premier temps de prohiber tout système d'identification de l'internaute connecté au réseau **(Section I)** mais d'organiser dans un second temps le nécessaire fichage des points d'accès au réseau **(Section II).**

Section I. La prohibition de tout système d'identification de l'internaute

257. **La prohibition de tout système d'identification de l'internaute.** Dans le monde physique les citoyens font l'objet d'un fichage via la carte nationale d'identité mais il ne peut jamais être établi de manière automatique une adéquation entre une personne physique et son état civil et il faut s'en garder. En dehors de la mise en œuvre de fichiers par les autorités de police, un tel système ne peut être généralisé dans un État de droit et en ce sens il faut aujourd'hui considérer l'encadrement des procédés de reconnaissance faciale.

Or sur le réseau, un système comparable à la carte d'identité ne peut être mis en œuvre alors qu'il ne s'agirait pas de s'enquérir d'un état civil mais d'identifier automatiquement l'internaute accédant au réseau via son adresse IP qui serait associé à ses coordonnées d'identité. Le contenu des débats ayant présidé à la mise en œuvre de la carte d'identité informatisée peut être repris. Dans son ouvrage *Histoire de la carte nationale d'identité* Pierre Piazza rappelle les craintes de la CNIL[534]et fait également état du fort mouvement de contestation de la société civile s'agissant de l'informatisation de la carte nationale d'identité[535].

Il a été démontré que le caractère automatique de la donnée IP n'en fait pas un identifiant de l'individu. Elle ne renvoie pas de manière univoque à une seule personne mais elle agit comme un signalement qui grâce à un procédé de déduction peut conduire à découvrir l'identité civile de l'internaute

[534] « De l'identité –« état civil » ne risque-t-on pas de passer insensiblement à la notion de système d'identification ? », peut-on lire dans lire dans son avis du 21 novembre 1979. Cette crainte l'incite alors à se prononcer en faveur de l'usage d'un numéro autorisant une identification de la carte nationale d'identité informatisée elle-même et non de son détenteur. Si la CNIL ne refuse pas que ce numéro mentionne le code du département de naissance du demandeur, elle souhaite que ce code soit uniquement suivi de chiffres ayant trait à la fabrication de la carte nationale d'identité informatisée. De plus, elle veut que ce numéro soit modifié à chaque renouvellement de la carte nationale d'identité informatisée. Estimant que ce document doit avoir pour seule finalité de permettre aux citoyens d'apporter la preuve de leur identité, la CNIL, suggère aussi de renoncer à l'idée d'utiliser une zone de lecture optique et des caractères ORC-B » ; V. : PIAZZA Pierre, *Histoire de la carte nationale d'identité,* Odile Jacob : Paris, 2004 (Odile Jacob histoire), p. 310, 312.

[535] Il cite les propos que tient le Centre d'information et d'initiative sur l'informatisation dans sa revue Terminal : « Si on se réfère à l'histoire des 40 dernières années, la police française a pourchassé, et toujours au nom de l'Ordre républicain ou national, les francs-maçons, les communistes, les Juifs, les résistants, les collabos, les partisans de l'indépendance de l'Indochine, puis de l'Algérie, les membres de l'OAS, les gauchistes, les terroristes. Imaginons un peu : si cette police avait fait « correctement » son travail à chaque fois, qui resterait-il aujourd'hui en France ? La démocratie exige ce minimum irréductible qu'on puisse faire de faux-papiers ». Pierre Piazza cite la revue *Terminal* n°2-3, janvier 1981, p. 20. V. : PIAZZA Pierre, *Histoire de la carte nationale d'identité, Odile Jacob : Paris, 2004 (Odile Jacob histoire), p. 310, 312.*

258. ***Plan.*** Ainsi d'une part le mécanisme d'adressage du réseau doit être respecté alors qu'il ne permet pas l'identification automatique de l'internaute à partir de l'adresse IP attribuée à sa connexion **(§1).** D'autre part il faut affirmer que l'internaute qui souhaite se connecter au réseau ne peut être requis de décliner son identité civile pour ce faire **(§2).**

§1) Le respect du mécanisme d'adressage du réseau

259. ***Plan***. L'internaute connecté doit pouvoir être retrouvé grâce à l'adresse IP attribuée à sa connexion mais ce uniquement dans le cadre d'une investigation nécessitant des moyens humains et ressortant des pouvoirs publics. Ainsi d'une part il faut sauvegarder la répartition dynamique des adresses IP alors qu'un internaute connecté ne doit pas pouvoir être identifié automatiquement par la seule interconnexion de ses données de connexion. **(A).** Toutefois alors que l'identification d'un internaute à partir de son adresse IP n'est jamais automatique il faut condamner tout procédé de masquage ou d'usurpation d'adresses IP qui ne peut relever que de prétentions libertaires alors que tout internaute doit pouvoir répondre de ses actions sur le réseau **(B).**

A] La sauvegarde de la répartition dynamique des adresses IP

260. ***Plan.*** A l'origine du réseau un mécanisme de répartition dynamique des adresses IP a été mis en œuvre alors que le protocole créé ne permettait pas un nombre suffisant d'adresses au regard des points de connexion du réseau. Aujourd'hui avec le protocole IPV6 tout point d'accès au réseau va pouvoir être doté d'une adresse fixe, autrement dit attribuée de manière pérenne dans le temps **(1).** Ce nouveau protocole pose une problématique s'agissant de l'identification de l'internaute connecté alors qu'il est désormais facile d'établir une adéquation entre une adresse IP circulant sur le réseau et le point de connexion qui l'a émise. Un nouveau mécanisme a ainsi été envisagé pour garantir que cette adéquation ne puisse pas être mise en œuvre par tout à chacun. **(2).**

1) Le nouveau protocole IPV6.

261. **Le mécanisme de la répartition dynamique des adresses IP.** Actuellement le protocole IPV4 ne permet pas qu'une répartition statique des adresses IP ait lieu entre tous les points d'accès au réseau. L'opérateur de communications est souvent obligé de répartir dynamiquement ses adresses IP. C'est-à-dire qu'il peut « *soit affecter exclusivement une adresse IP de sa collection à un abonné, l'adresse IP restera alors valable tant que ce client restera abonné à ce fournisseur d'accès. Il peut également redistribuer celles-ci dynamiquement, en admettant que statistiquement tous ses clients ne sont pas connectés en*

même temps. Il peut ainsi gérer un plus grand nombre d'abonnés que d'adresses IP achetées »[536].

Cette répartition dynamique est révélatrice de l'ambiguïté de l'adresse IP dont le caractère identifiant dépend des données qui peuvent lui être associées et dépend donc des acteurs qui les détiennent. En effet la répartition dynamique fait apparaître qu'une même adresse IP peut être allouée à deux points d'accès différents à des moments différents. Une même adresse IP visible à des moments différents sur le réseau ne peut être considérée comme appartenant au même point d'accès. Ainsi actuellement l'attribution d'une adresse IPV4 ne peut se départir d'un rapport au temps : c'est l'adresse fournie à un point d'accès à un moment « *t* » donné. Seul l'accès aux informations détenues par l'opérateur de communications électroniques et l'administrateur réseau peut permettre de considérer la localisation du point d'accès.

262. **Le nouveau protocole IPV6**. Toutefois en raison du développement de l'accès à internet, notamment dans les pays émergents, et de la multiplication des connexions, notamment à travers le développement de ce que l'on appelle l'internet des objets, un tel mécanisme de répartition dynamique arrive à son point de rupture[537]. Un nouveau protocole dit « IPV6 » a été mis en œuvre qui permet de multiplier de manière telle le nombre d'adresses disponibles que cette problématique d'une adresse IP envisagée comme une ressource n'est aujourd'hui plus d'actualité[538].

Si la transition du protocole IPV4 vers l'IPV6 est encore laborieuse, le mécanisme d'adressage du réseau s'oriente toutefois vers une nouvelle répartition des adresses qui sera fixe. Techniquement tout point d'accès au réseau sera doté d'une adresse unique et pérenne dans le temps. Or ce nouveau procédé fait apparaître les dangers d'un fichage des points de connexion en regard des adresses IP qui leurs sont attribuées. Ce fichier de données qui pourrait porter le nom d'annuaire ne doit pas être public et accessible à tous. La dynamique de répartition des adresses IP doit être sauvegardée de manière à ce qu'une adresse IP visible sur le réseau ne puisse pas être, facilement et publiquement, reliée à un point d'accès physique du réseau.

[536] Définition de l'IP fixe sur www.dicodunet.com

[537] V. l'entrée « épuisement des adresses IPV4 » sur le site wikipédia.org

[538] « Appelé par les spécialistes « IPV6 » la version 6 du protocole Internet qui intègre des adresses IP de longueur bien supérieure, difficilement imaginable à l'échelle humaine : « 3,4 par 10 puissance 8 ou encore 667 millions de milliards d'adresses par millimètre carré de surface terrestre (même si toutes ces adresses ne seront pas utilisables sur Internet) », v. DESGENS-PASANAU G., FREYSSINET E., L'identité à l'ère numérique, Paris : Dalloz, 2009 (Presaje), p. 87.

2) Le mécanisme de l'« IPV6-privacy ».

263. **L'enjeu du protocole IPV6 eu égard à l'identification de l'internaute**. La fixité des adresses IP facilite le procédé d'identification de l'internaute connecté au réseau et ce d'autant plus avec la démocratisation de l'internet des objets.

En effet si tout point de connexion a une adresse unique ainsi que les objets qui se connectent à lui, des schémas de connexion apparaissent qui révèlent l'usage du point d'accès[539]. Autrement dit la collecte d'une adresse IPV6 par toute personne peut conduire à partir d'un procédé de déduction se basant uniquement sur les données produites par l'utilisation du réseau à l'identification de l'internaute connecté. Il pourrait y avoir identification automatique alors que celle-ci serait réalisée uniquement à partir de données numériques.

Par exemple un internaute pourrait considérer l'adresse IP d'un individu qui vient de lui écrire un courriel et réaliser quelques jours plus tard que cette adresse est également celle du commentaire peu élogieux qui a été fait sur son blog via un pseudonyme.

264. **Le mécanisme dit « *IPV6-privacy* ».** Pour répondre à ces inquiétudes un mécanisme dit d'« *IPV6-privacy* » a été prévu pour réintroduire une dynamique de répartition. A l'adresse IPV6 fixe de l'abonnement, connue seulement du FAI et de l'abonné, est associée de manière aléatoire et temporaire (1 ou 2jours) une autre adresse IPV6 qui, elle, est visible sur le réseau (on dit qu'elle est routable)[540].

Ainsi une adresse IP visible sur le réseau ne peut jamais être associée de manière univoque à un point d'accès au réseau et conduire si les données d'adressages se multiplient à l'identification de l'internaute connecté. Un procédé d'investigation est nécessaire pour considérer qui est à l'origine de la connexion. Cette logique conduit à condamner l'utilisation d'un logiciel de masquage de l'adresse IP alors que celle-ci ne permet jamais d'identifier automatiquement l'internaute connecté.

B] La prohibition des logiciels de masquage de l'adresse IP

[539] Comme le souligne G.Desgens-Pasanau et G.Freyssinet «chaque être humain disposera potentiellement d'une adresse IP mais aussi chacun des objets qui nous entourent pourra être connecté. Et ce qui est particulièrement fort en termes d'identification, c'est que vraisemblablement les règles de définition de ces adresses imposeront que chacune d'entre elle soit associée à un numéro racine (un bloc) qui sera associé à un abonné Internet et donc lorsque ces objets communiqueront avec les autres, il en résultera d'autant plus d'opportunités d'identifier l'internaute qui en est responsable ».

[540] V. sur le site « Comment ça marche.Net », le forum « réseau » et sa discussion intitulée « comprendre l'adressage IPV6 », www.commentçamarche.net

265. ***Plan.*** La possibilité d'identifier l'internaute connecté doit s'envisager à la marge d'un usage non dévoyé du réseau qui est en premier lieu un espace d'épanouissement de toutes les libertés individuelles. Pour profiter de l'usage de celles-ci, l'individu doit pouvoir être identifié. Le principe doit être que tout usage d'un logiciel comme *TOR* ou *iPredator* qui masque une adresse IP soit condamné **(1)**. La difficulté une fois le principe défini est de considérer dans quelle mesure il peut être mis en œuvre **(2)**.

1) Le principe d'une telle prohibition

266. **Le fonctionnement d'un logiciel de masquage tel TOR**. Le réseau TOR (pour *The Onion Router)* est un réseau informatique superposé qui permet de masquer l'adresse IP à l'origine de la connexion[541]. L'adresse IP emprunte en effet un chemin composé de nœuds qui n'appartiennent pas au réseau mondial et qui ont la particularité de modifier l'adresse IP au fur et à mesure de sa progression. L'adresse qui sort du dernier nœud et qui cherche à se connecter au site web n'est pas celle attribuée à l'origine à la connexion[542]. Le site web constate que l'adresse provient du réseau TOR mais il est très difficile de remonter à l'adresse d'origine.

Ce projet d'un réseau permettant de rendre anonymes les connexions, au sens de rendre impossible toute identification de l'internaute, est né d'une volonté de se protéger contre une certaine forme de surveillance sur internet et contre ce que l'organisation à l'origine du logiciel appelle « *l'analyse de trafic* »[543]. La défense de la vie privée est invoquée alors que l'usage de TOR empêche tout suivi de la navigation de l'internaute et toute géolocalisation, alors que l'adresse physique de connexion de celui-ci ne peut être retrouvée[544]. En Suède, les créateurs du site *The Pirate Bay* ont pour leur part créé un service aux mêmes fins s'appelant *ipredator*.

Cette revendication peut tout à fait être entendue. Toutefois la solution proposée n'est pas valable en ce qu'elle pose le problème à l'envers : au lieu de remettre en cause les procédés de surveillance et de tenter d'organiser un régime légal visant à encadrer ceux-ci, la position adoptée est de se cacher. Cette posture est condamnable en ce qu'elle ne souffre pas de nuances ; elle sous-entend nécessairement que le réseau ne peut s'apparenter à un État de droit et qu'il est légitime de ne pas apparaître à visage

[541] V. l'entrée « TOR (réseau) » sur le site wikipédia.org

[542] Telles les couches d'un onion, les différents nœuds ont emprisonnés le protocole inital, d'où le nom de ce réseau

[543] V. le site www.torproject.org, et le slogan de sa page d'accueil « *Anonymity online. Protect your privacy. Defend yourself against network surveillance and traffic analysis* ».

[544] Ibid.

découvert sur celui-ci. Ce manichéisme ne peut conduire qu'à des prétentions libertaires et non protectrices des libertés.

267. **L'exigence du maintien de l'ordre public**. Il serait tentant de comparer la prohibition de tels logiciels à l'interdiction générale posée par la loi n°2010-1192 du 11 octobre 2010 qui énonce dans son article 1er : « *Nul ne peut, dans l'espace public, porter une tenue destinée à dissimuler son visage* »[545]. Toutefois cette généralité de l'interdiction qui a fait couler beaucoup d'encre ne sied pas à notre approche[546].

En effet l'interdiction de la dissimulation de l'adresse IP ne répond pas en premier lieu[547] des « *exigences minimales de la vie en société* »[548] qui se réfèrent à un ordre public immatériel. Il ne s'agit pas ici de consacrer : « *le droit de dévisager et l'obligation d'être dévisagé* »[549] mais bien d'abord au nom du maintien de l'ordre public dans ses composantes matérielles, -de tranquillité, de salubrité et de sécurité publique-, de permettre le dévoilement du visage à des fins d'identification.

En effet dans un État de droit un individu doit pouvoir se soumettre à un contrôle d'identité, les conditions de celui-ci étant par ailleurs légalement définies[550]. Et ainsi on ne peut envisager le port d'un vêtement dissimulant le visage, en dehors des cas relevant de l'expression d'une religion ou d'une opinion, que comme témoignant d'une volonté de nuisance. Si les tenants du projet TOR mettent en avant leur choix, qui est de fait ici non pas religieux mais politique, de ne pas se soumettre à une surveillance qu'ils estiment généralisée et attentatoire à leurs libertés, ce point de vue ne peut masquer la possibilité première qu'offre un tel logiciel qui est celle de permettre à ses utilisateurs de se cacher et dès lors de se livrer à des activités illégales se sachant à l'abri de toutes poursuites. Ainsi le logiciel TOR est utilisé sur les réseaux superposés constituant le « *Darknet* »[551]. Ces réseaux de type pair-à-pair ont pour vocation la mise en relation

[545] Loi n°2010-1192 du 11 octobre 2010 interdisant la dissimulation du visage dans l'espace public.

[546] VERPEAUX M. « Dissimulation du visage, la délicate conciliation entre la liberté et un nouvel ordre public, *AJDA* 2010, 2373 ; DIEU F. « Le droit de dévisager et l'obligation d'être dévisagé : vers une moralisation de l'espace public ? », *JCP adm.* 2010, 2355 ; LEVADE A., « Epilogue d'un débat juridique : l'interdiction de la dissimulation du visage dans l'espace public validée, *JCP G* 2010, 1043. Sur les circulaires relatives à la mise en œuvre de la loi, v. : LEROYER A.M., « La circulaire et le voile : interrogations sur une notion émergente : « Les exigences minimales de la vie en société », *RTD civ.*, 2011, p.399 ; DIEU F., « Dissimulation du visage : la confirmation d'un interdiction de large portée-à propos des circulaires du 2 mars 2011 et du 31 mars 2011, *JCP adm.*, 2011, 2144.

[547] Car dans un second temps, il pourrait être argué que l'usage de ce logiciel libre qu'est TOR relève de l'affirmation d'une opinion.

[548] V. la décision du Conseil constitutionnel du 7 octobre 2010, DC n°2010-613, cons. 4.

[549] DIEU F. « Le droit de dévisager et l'obligation d'être dévisagé : vers une moralisation de l'espace public ? », *JCP adm.* 2010, 2355

[550] V. l'article 78-1 du CPP.

[551] V. l'article consacré au « Darknet» sur le site fr.wik/ipédia.org

d'individus qui souhaitent faire le commerce de choses illicites et qui permettent également le partage de fichiers illicites telles des images pédophiles par exemple[552].

Une fois le principe établi d'interdire à l'internaute de masquer son adresse IP ou d'usurper celle d'un tiers, la difficulté est en réalité de considérer dans quelle mesure ce régime peut être mis en œuvre.

2) La difficile mise en œuvre de sanctions pénales

268. **La mise en œuvre d'une telle interdiction**. Deux pays ont par le passé mis en œuvre des actions à l'encontre du logiciel TOR. Ainsi d'une part en 2014 le ministère de l'intérieur en Russie à offert une soumission de 3,9 millions de roubles (environ 85000€) à tout projet de recherche visant à percer le chiffrage du logiciel[553]. Cette somme dérisoire au regard du travail à mettre en œuvre pour trouver une faille dans le système révèle en réalité une position politique[554]. D'autre part, la même année, la justice autrichienne a condamné un homme mettant à disposition un nœud sur le réseau TOR à trois ans de contrôle judiciaire et 30000 euros d'amende, le jugeant complice des actions criminelles dont il a permis la réalisation en fournissant un moyen d'anonymisation des connexions[555]. Toutefois il a été souligné que cette décision était d'espèce au regard du profil de hacker de l'accusé et qu'elle ne pouvait être considérée comme une interdiction générale du logiciel.[556]

La difficulté apparaît à cet endroit : en effet il est difficile de condamner la technologie d'anonymisation en elle-même qui est nécessaire par exemple dans les pays où la démocratie est menacée par des politiques de « *real name* » notamment ou des blocages arbitraires de sites[557], pour que les journalistes ou les dissidents politiques puissent communiquer. De la même manière que l'on ne peut *de facto* considérer comme condamnable le mécanisme d'identification de l'internaute via son adresse IP permis sur le réseau car des politiques autoritaires y sont menées, on ne peut anéantir dans une société démocratique la possibilité d'échapper à toute identification, même si cette possibilité permet la criminalité. L'action n'a pas à être menée contre le logiciel

[552] L'exemple peut être pris du réseau « Silk road » autrement appelé le « eBay de la drogue » et qui a été fermé en 2013 par les autorités américaines. V. BALL J, ARTHURAND C., GABATT A., « FBI claims largest Bitcoins Seizure after arrest of Silk Road founder", article mis en ligne le 2 octobre 2013 sur le site theguradian.com.

[553] LUHN A., "Russia offers 3.9m roubles for ´research to identify users of TOR´", article mis en ligne le 25 juillet 2014 sur le site theguardian.com.

[554] Ibid.

[555] JARVINEN H., « Russia and Austria take action against the use of TOR", article mis en ligne le 30 juillet 2014 sur le site de l'association EDRI (European Digital Rights), edri.org.

[556] Ibid.

[557] Il est à noter que la volonté de bloquer l'usage de TOR en Russie faisait ainsi suite à une augmentation de l'utilisation de ce réseau alors que le gouvernement venait de mettre en œuvre une politique dite de « real name » pour tout contributeur d'un site ayant plus de 3000 visiteurs par jour et que les blogs de plusieurs dissidents politiques venaient d'être bloqués. V. LUHN A., "Russia offers 3.9m roubles for ´research to identify users of TOR´", article mis en ligne le 25 juillet 2014 sur le site theguardian.com.

libre et l'organisation qui en est à l'origine. C'est l'usage de celui-ci qui doit être sanctionné.

269. **La régulation opérée par les sites du web.** Il peut d'abord être noté qu'une régulation peut s'opérer s'agissant des connexions mises en œuvre à partir d'un nœud TOR.

En effet alors que le site vers lequel s'oriente la connexion est à même de visualiser que celle-ci a emprunté le réseau d'anonymisation, il peut bloquer la connexion. Ainsi le site *Wikipédia.org* empêche qu'une telle adresse crée ou modifie un contenu sur son service[558]. Toutefois il faut souligner que la tendance aujourd'hui est plutôt inverse : les géants du web permettent aux utilisateurs qui le souhaitent de se connecter à leurs services à partir d'une adresse IP émise par le logiciel TOR. L'exemple du réseau social Facebook peut être cité qui a lancé cette fonctionnalité en 2014 alors que précédemment l'entreprise californienne indiquait bloquer de telles adresses.

Le paradoxe n'a pas manqué d'être souligné : alors que Facebook met en garde sur l'utilisation de pseudonymes pour créer un compte, il conçoit que ses utilisateurs puissent ne pas être identifiés par des tiers. L'entreprise a mis en avant la volonté de permettre à la marge la sécurité des connexions de certains utilisateurs qui souhaiteraient échapper à la surveillance et la censure de certains régimes autoritaires. Runa Sandvik, ancien développeur du réseau TOR, affirme ainsi que TOR tend à devenir une option de confidentialité qui devrait se généraliser pour d'autres entreprises du numérique[559].

Il faut condamner cette assertion. La régulation opérée par les sites du web ne peut être que marginale et ne résout pas la problématique qui doit viser de manière générale cette volonté de ne pas être identifié.

270. **Les sanctions pénales à mettre en œuvre**. La sanction de la falsification d'une adresse IP fait apparaître un nœud gordien. En effet l'individu à sanctionner doit pour cela être retrouvé. S'il n'est pas impossible de retrouver un utilisateur de TOR, et ces investigations s'imposent même dans le cas de la lutte contre la cybercriminalité, la question qui se pose alors est celle de l'utilité d'une sanction visant le procédé d'anonymisation en sus de celle de l'infraction réalisée.

[558] V. l'entrée « TOR (réseau) », rubrique « blocage de TOR » sur le site wikipédia.org.

[559] « Why Facebook just launched its own 'Dark web' site », article mis en ligne sur le site du mensuel américain, *Wired*, le 3 novembre 2014.

Le choix coercitif aurait pu être celui d'une circonstance aggravante alors que toutes les infractions ne sont pas commises par le biais d'adresses IP falsifiées ; une telle pratique a de fait été considérée dans les premiers temps du réseau comme constitutive de la mauvaise foi de l'internaute pour les infractions qui la nécessitaient[560]. En 2011, la loi d'orientation et de programmation pour la performance de la sécurité intérieure dite « LOPPSI II » a créé l'article 226-4-1 du Code pénal qui sanctionne le délit d'usurpation d'identité en lui-même. L'infraction créée recouvre l'usurpation « *d'une donnée de toute nature* » ; de plus la réalisation d'un tel délit sur « *un réseau de communication au public en ligne* » est expressément prévue. L'usurpation de l'adresse IP d'un tiers est donc sanctionnée en tant que telle désormais. Une infraction qui laisse toutefois en suspens la question de la sanction de l'utilisation d'un logiciel comme TOR qui rend anonyme une adresse en lui en substituant une nouvelle adresse IP qui n'est pas celle d'un tiers mais qui est issue des propres nœuds mis en œuvre par le logiciel.

Ainsi il apparaît qu'en définitive la lutte contre la falsification des adresses IP sur le réseau relève en réalité des services de polices et de leur capacité à déjouer les mécanismes mis en œuvre par les délinquants. Il s'agit d'abord de considérer que l'usage du réseau n'est pas nécessairement dévoyé et d'envisager comment à partir d'une adresse IP valide peut être retrouvé l'individu à l'origine de la connexion. Pour ce faire il faut définir le contenu du régime à mettre en œuvre par les pouvoirs publics pour pouvoir identifier l'internaute connecté à partir de cette adresse.

§2) L'interdiction de requérir l'identité civile de l'internaute souhaitant se connecter au réseau

271. ***Plan.*** Il faut affirmer que ne saurait être mis en œuvre un système d'identification préalable de tout internaute connecté au réseau ; l'identité civile de l'internaute ne peut être requise pour accéder au réseau et se voir attribuer une adresse IP. Aucune adresse IP circulant sur le réseau ne doit pouvoir être associée à un document d'identité ; serait alors méconnu le droit d'accès alors que l'internaute doit être libre de se connecter anonymement **(A)**. En revanche dans le cadre d'un sous-réseau étendu qui vise une collectivité définie, des droits d'accès qui individualisent chaque connexion peuvent être mis en œuvre alors qu'il est légitime que l'internaute soit, à cet endroit, autorisé à se connecter **(B).**

A] L'atteinte à la liberté d'accès au réseau

[560] Dans le cas de l'utilisation malveillante d'un nom de domaine, l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) a toutefois considéré que si l'usage d'un proxy rendant anonyme l'adresse IP pouvait être considéré comme un indice de mauvaise foi, cet indice restait insuffisant en l'absence d'autres éléments prouvant la fraude. V. WIPO Arbitration and Mediation Center, Administrative panel decision, November 12, 2006 (Case No. D2006-1214).

272. **L'enjeu des nouveaux modes d'accès au réseau**. Alors qu'il est nécessaire de pouvoir identifier toute personne à l'origine d'un délit, il est souvent fait état des difficultés que pose le réseau qui ne met en relation que des données numériques dont la nature personnelle est questionnée.

De fait le procédé d'adressage du réseau est complexe et peu compris. Si l'on conçoit l'identification d'un internaute connecté à partir d'une adresse IP attribuée au domicile d'un particulier, la mise à disposition d'un accès au public élargit le champ d'investigation s'agissant de l'internaute connecté. Au début des années 2000, le cas des cybercafés est abondamment cité ; au tournant des années 2010, dans le cadre notamment des débats sur la loi Création et Internet dite « HADOPI », les députés de l'opposition soulignent l'enjeu des nouveaux modes d'accès au réseau qui renvoient à la multiplication des points wifi mis à disposition non plus seulement dans le cadre d'une activité principale mais de manière générale par de nombreux commerces et lieux ouverts au public, comme des collectivités territoriales, telle par exemple la ville de Paris[561].

Il faut, s'agissant de ces accès mis à disposition du public, affirmer qu'il serait liberticide d'exiger de l'internaute souhaitant s'y connecter un document d'identité. L'identification de l'internaute souhaitant se connecter au réseau ne peut renvoyer au système d'identification mis en œuvre dans le monde physique **(1).** En revanche cette prohibition n'empêche pas la collecte d'informations sur l'internaute qui peut être contraint à la divulgation d'informations le concernant pour bénéficier de cet accès au réseau **(2).**

[561] Lors de l'audition de Mme la ministre Christine Albanel devant la Commission des lois constitutionnelles de la législation et de l'administration générale de la République, le mardi 17 février 2009, Christian Paul, député PS, interpelle la ministre en ces termes : « *Comme l'indique une note récemment publiée par le ministère des finances – vous voyez que je suis très éclectique dans mon usage des sources –, il existe à Paris des centaines de bornes Wi-Fi, qui permettront de continuer à télécharger gratuitement des fichiers musicaux. Pour cela, il suffira de se rendre chez McDonald. Ce texte repose donc sur une illusion sécuritaire.* » V. compte-rendu n°27 disponible sur le site de l'Assemblée Nationale. http://www.assemblee-nationale.fr/13/cr-cloi/08-09/c0809027.asp

Lors de l'examen du projet de loi, adopté par le Sénat favorisant la diffusion et la protection des œuvres sur Internet, devant la commission des lois constitutionnelles de la législation et de l'administration générale de la République, le mercredi 18 février 2009, Patrick Bloche s'interroge sur l'applicabilité du projet de loi en ce qu'il concerne les personnes morales : « *Il convient de limiter les mécanismes de responsabilité juridique prévus dans cet article aux seules personnes physiques, afin d'éviter de lourdes conséquences pour les collectivités locales, les bibliothèques, les écoles ou les entreprises qui offrent un accès à internet. Qu'adviendra-t-il dans ces conditions, des accès à internet offerts pas de nombreuses communes, telles que la ville de Paris par le biais des réseaux wi-fi?* » V. compte-rendu n°28 disponible sur le site de l'Assemblée Nationale : http://www.assemblee-nationale.fr/13/cr-cloi/08-09/c0809028.asp

1) Le caractère liberticide d'une requête de documents d'identité

273. **L'identification des clients de cybercafés : l'exemple de la législation italienne**. S'il a pu être considéré au début des années 2000 en France de requérir les documents d'identité de tout client de cybercafé, cette voie n'a heureusement pas été suivie et il faut s'en féliciter. Quand bien même l'individu ne se connecte pas depuis son domicile qui lui garantit un espace d'intimité, il ne peut être obligé d'attester de son identité pour se connecter au réseau.

Ainsi il faut fermement condamner la législation italienne qui a exigé des responsables des cybercafés qu'ils requièrent les documents d'identité de leurs clients. Le décret-loi dit « Pisanu » du 16 Août 2005[562] impose à toutes les personnes mettant à disposition un accès au public qu'elles exigent de leurs clients ou utilisateurs un document d'identité[563]. De fait cette disposition a été abrogée en 2013[564].

274. **Le non-sens de telles politiques, désormais désuètes**. En réalité cela était déjà souligné à l'époque, cette problématique des services mis en œuvre par des cybercafés était contextuelle et marginale.

Le conseiller à la Cour de cassation, Pierre Leclerq soulignait déjà en 2008, dans un colloque organisé par le CEJEM intitulé « *Banque et Internet* », que les individus se croyant plus à l'abri de poursuites derrière l'ordinateur d'un cybercafé se trompent dès lors qu'aux serveurs de tels commerces sont attribuées des adresses IP fixes ; le lien entre celles-ci et le lieu de connexion est ainsi beaucoup plus rapide pour les enquêteurs[565]. Cette fixité des adresses IP d'un cybercafé permet une plus grande visibilité des connexions établies et une surveillance accrue des pouvoirs publics. Par ailleurs le gérant du cybercafé établit nécessairement un contact physique avec son client qui doit payer le service et auquel il attribue un ordinateur ou un point d'accès.

Aujourd'hui la logique de l'adresse IP est mieux comprise et il apparait que l'investigation s'agissant de l'identité civile de l'internaute connecté renvoie à la conservation d'une trace de l'attribution d'une adresse IP à un point d'accès au réseau,

[562] V. Decreto 16 agosto, 2005, (Pubblicato sulla Gazzetta Ufficiale n. 190 del 17-8-2005), "Misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso a Internet utilizzando tecnologia senza fili, ai sensi dell'articolo 7, comma 4, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155. (GU n. 190 del 17-8-2005)"

[563] V. ibid, Articolo 1, 1. « b) identificare chi accede ai servizi telefonici e telematici offerti, prima dell'accesso stesso o dell'offerta di credenziali di accesso, acquisendo i dati anagrafici riportati su un documento di identità, nonché il tipo, il numero e la riproduzione del documento presentato dall'utente; »

[564] V. la loi de conversion n°98/2013, Gazzetta Ufficiale, n°194, 20 agosto 2013.

[565] « Banque et Internet », colloque organisé par le CEJEM, le jeudi 11 juin 2008.

autrement dit à un fichage des points d'accès au réseau[566]. Toutefois cette prohibition de requérir un document d'identité n'empêche pas de collecter des informations auprès de l'internaute visant à l'identifier alors que les points wifi se multipliant, le contact physique avec le titulaire du point d'accès au réseau est de plus en plus ténu.

2) La collecte d'informations visant l'identification de l'internaute connecté

275. **Le développement des bornes wifi**. Aujourd'hui l'accès à une connexion internet filaire[567], en dehors du domicile, peut se faire dans un nombre considérable de lieux alors que la mise à disposition d'une borne wifi est envisagée comme un service nécessaire à proposer à ses clients ou visiteurs. Ainsi en tout lieu, que ce soit un restaurant, un hôtel, un aéroport par exemple, et même plus généralement dans les parcs et rues de Paris, il est possible d'obtenir une connexion wifi.

Le service est souvent gratuit car il apparaît comme l'accessoire de l'activité principale de l'établissement. Le client doit consommer pour obtenir un code d'accès au réseau mis en œuvre, ce qui *a minima* permet le lien physique avec un individu identifié qui est par ailleurs visible par toutes les personnes à proximité du point d'accès.

Toutefois de plus en plus, notamment dans le cadre de bornes d'accès couvrant un territoire et non associées à un service, comme par exemple celles de la ville de Paris, il n'est pas de lien direct entre l'internaute connecté et le titulaire de l'abonnement ou un de ses employés. Il est alors tout à fait légitime de mettre en œuvre des formulaires d'identification à remplir pour pouvoir se connecter.

276. **Le contenu des formulaires d'identification**. La mise en œuvre d'un formulaire d'identification ne s'apparente pas à une limite du droit d'accès au réseau qui doit être garanti à tout individu.

En effet il ne procède pas d'un mécanisme visant à autoriser l'internaute à se connecter. Dans le cadre de la mise à disposition d'un réseau wifi à un public indéterminé, une collecte d'informations est mise en œuvre mais elle ressort de la volonté de l'internaute. L'internaute est libre de remplir le formulaire comme il le souhaite. La collecte d'informations vise la responsabilisation de l'internaute qui va utiliser une connexion qui n'est pas celle dont il est titulaire et qui doit pour se faire s'identifier.

[566] *V. infra.* Section II : « *Le nécessaire fichage des points d'accès au réseau* ».
[567] Entendu ici en opposition à l'accès cellulaire pouvant se faire à partir du téléphone portable et du réseau 4G.

Ainsi la ville de Paris par exemple dans son portail d'accès invite l'utilisateur à renseigner ses « *nom, prénom et e-mail* » et à accepter les conditions générales d'utilisation. L'utilisateur peut alors tout à fait utiliser des données révélant un pseudonyme. Par ailleurs la requête d'une adresse de courriel permet une interaction avec l'utilisateur et un lien avec d'autres coordonnées détenues par le fournisseur de celle-ci, dont la divulgation toutefois doit être encadrée.

Ainsi il ne s'agit pas d'un procédé d'authentification qui met en œuvre des droits d'accès visant à considérer les connexions d'un public défini autorisé à se connecter à un réseau local.

B] La possible authentification de l'internaute connecté

277. **La logique d'un procédé d'authentification.** Le rôle de l'adresse IP dans l'identification de l'internaute doit être parfaitement saisi : c'est la seule donnée qui permet d'attester[568] de l'identité d'un internaute connecté au réseau et naviguant sur celui-ci, en ce qu'elle garantit le lien avec la réalité. En effet elle seule renvoie à un élément intangible du monde physique : la localisation du point d'accès utilisé. Il faut affirmer ainsi qu'il ne peut être attesté qu'un individu est à l'origine d'une connexion litigieuse en dehors du constat de sa présence physique derrière la machine servant de point d'accès ou à proximité de celle-ci dans le cas d'un accès au réseau mis en œuvre par un signal wifi.

Il faut considérer la différence entre cette identification permise par l'adressage du réseau et le procédé d'authentification de l'utilisateur d'un réseau local qui vise en réalité à autoriser un individu à se connecter **(1).** L'exemple du contentieux opposant les établissements bancaires à leur clients s'agissant des procédés d'identification de l'individu à l'origine d'un ordre de paiement permet de considérer le sens d'un tel procédé : l'authentification permet simplement de considérer que l'accès au réseau local est légitime en ce qu'il s'opère avec un nom d'utilisateur et un mot de passe qui sont reconnus par l'administrateur du réseau **(2).**

1) La mise en œuvre de droits d'accès au réseau

278. **Le contenu des droits d'accès au réseau**. Une entité, comme une entreprise ou une université, peut créer un sous-réseau dans le but de mettre à disposition un accès au réseau mondial à la collectivité qu'il vise. Ce sous-réseau permet souvent également la mise à

[568] V. l'entrée « Attester » : « Attester v.t. (lat. *attestari*, de *testis*, témoin). 1. Certifier la vérité ou l'authenticité de : *J'atteste qu'elle a dit la vérité », in* Le Petit Larousse illustré, Paris : Larousse, 2015. V. également cette même entrée : « Attester : *2.sens usuel* : Témoigner de la vérité, de la réalité de quelque chose. », sur le site du Centre National de Ressources Textuelles et Lexicales, www.cnrtl.fr

disposition via des serveurs propres à des ressources et services communs, comme une messagerie, un intranet ou un espace numérique de travail.

L'administrateur d'un réseau local peut alors conditionner l'accès de celui-ci à un nom d'utilisateur et un mot de passe qu'il a lui-même choisis et qui peuvent consister en un nom et prénom de l'individu. En effet il faut considérer que dans le cadre d'un réseau local, l'administrateur réseau peut s'assurer que celui-ci n'est utilisé que par les personnes autorisées, comme les salariés d'une entreprise ou les personnels et étudiants d'une université, en mettant en œuvre des droits d'accès, qui consistent en des données choisies par lui et qui doivent authentifier l'internaute qui souhaite se connecter.

279. **La logique de la mise en œuvre de droits d'accès au réseau**. Il faut souligner toutefois que quand bien même les informations portent sur des éléments d'identification de l'internaute, ces seules données ne peuvent attester de la présence physique de l'internaute et de sa connexion au réseau. La logique est celle du recoupement d'informations. La mise à disposition du nom d'utilisateur et du mot de passe à l'origine de la connexion au réseau local ne permettent à elles seules aucune investigation efficace s'agissant de l'individu connecté. Le pré-requis est la localisation du point d'accès utilisé grâce à l'adresse IP. L'authentification est le fait de données et ne ressort pas d'une investigation. Elle ne peut se juxtaposer avec l'identification de l'internaute connecté quand bien même elle peut être très forte[569]. Seule la localisation du point d'accès utilisé couplée avec le contenu des droits d'accès ou des informations requises à la création du compte-utilisateur permet sensiblement de restreindre le champ des recherches.

2) La logique d'un tel procédé : l'exemple de l'identification d'un individu à l'origine d'un ordre de paiement

280. **Le contentieux de l'identification de l'individu à l'origine d'un ordre de paiement**. L'exemple peut être pris des prescriptions du Code monétaire visant à définir les conditions qui permettent à un établissement de crédit de prouver qu'une opération de paiement contestée a bien été « *authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre* »[570].

[569] On pourra souligner d'ailleurs à cet endroit que tout procédé d'authentification, de par son automatisme, peut être faillible. On citera l'exemple presque courant de tous les scénarii du genre de la « dystopie » : l'œil ou la main d'une personne peuvent être utilisés par un tiers.

[570] Article L133-23, alinéa 1, du code monétaire et financier.

L'article L123-23 alinéa 2 de ce code précise en effet que « *l'utilisation de l'instrument de paiement telle qu'enregistrée par le prestataire de services de paiement ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière* ». Autrement dit la composition du code confidentiel à quatre chiffres ou l'indication des identifiants de la carte bancaire dans le cas d'un paiement en ligne ne permettent pas d'affirmer que l'ordre a bien été passé par le client de la banque, ni qu'il s'est rendu coupable d'une fraude ou d'une négligence grave alors qu'il doit veiller à la confidentialité de ces informations. L'authentification d'une transaction n'équivaut pas à l'identification de la personne à l'origine de celle-ci et il faut considérer qu'un vol de données ait pu avoir lieu. Dès lors, dans la pratique, les établissements bancaires ont argué du fait que l'ordre de paiement avait été donné depuis le domicile du client en relevant l'adresse IP à l'origine de la connexion. Ce mode de preuve qui a été reçu[571], est contesté ; la possibilité d'usurpation d'une adresse IP est dénoncée[572].

281. **L'indication clef : l'adresse IP à l'origine de la connexion.** Toutefois le raisonnement à tenir n'est pas de considérer en premier lieu le caractère numérique de l'adresse IP et dès lors sa possible usurpation, mais d'envisager d'abord son incidence dans un processus de recoupement d'informations dans le but de renverser la charge de la preuve. Les identifiants d'une carte bancaire couplés à un code confidentiel ne peuvent attester que l'ordre de paiement est le fait du titulaire de la carte. Ces identifiants mis en œuvre à partir d'une adresse IP attribuée au point de connexion de son domicile ne permettent toujours pas d'attester de la présence physique de l'internaute et de sa volonté de réaliser la transaction, toutefois la réunion de ces éléments peut permettre de renverser la charge de la preuve alors qu'il est difficile de considérer l'utilité pour l'usurpateur de mettre en œuvre à la fois le vol des données bancaires et le « *spoofing* »[573] de l'adresse IP du titulaire de la carte alors que le masquage de son adresse IP suffit à le rendre anonyme.

L'adresse IP de par la technicité qui la caractérise est une donnée que l'on peut considérer comme plus tangible que des codes d'accès alors qu'elle renvoie à la structure même du réseau. Elle peut tout aussi être usurpée mais alors il ne s'agit pas de voler des codes mais d'agir sur le mécanisme même d'adressage du réseau, qui est

[571] Metz, 8 Décembre 2010, *L'essentiel du Droit Bancaire,* fév. 2011, p. 6, obs J. Lasserre-Capdeville

[572] J.Lasserre-Capdeville, « Les problèmes liés à l'adresse IP en matière bancaire *Dalloz IP/IT*, 219, avril 2017

[573] Le mot *spoofing* est un terme anglais qui signifie « usurpation » ou « parodie » parfois utilisé en informatique pour désigner l'usurpation d'adresse IP (*IP spoofing*). V. l'entrée « spoofing » sur le site wikipédia.org.

technique et volatile. De fait il convient au regard de ce procédé automatique d'organiser un fichage des points d'accès auxquels ont été attribuées les adresses IP pour permettre une investigation efficace s'agissant de l'identification de l'internaute connecté.

Section II. Le nécessaire fichage des points d'accès au réseau

282. **Le nécessaire fichage des points d'accès au réseau utilisé**. Pour pouvoir retrouver un individu à partir d'une adresse IP visible sur le réseau, il est nécessaire de pouvoir rattacher celle-ci à un point d'accès localisé physiquement.

En effet il a été montré que c'est cette indication d'un lieu physique de connexion qui permet une investigation efficace. C'est elle qui permet de déterminer qui était présent physiquement derrière l'ordinateur servant de point d'accès ou à proximité de celui-ci si la connexion au réseau est mise en œuvre par un signal wifi. Ainsi toute personne qui attribue à une machine une adresse IP pour qu'elle puisse être connectée à l'internet doit être à même de considérer au regard de cette adresse un lieu physique de connexion. Une concordance doit toujours pouvoir s'établir entre une adresse IP visible sur le réseau et le point d'accès auquel elle a été attribuée.

L'opérateur de communications électroniques peut faire le lien entre une adresse IP relevée sur le réseau et la boucle finale d'accès au réseau d'un de ses abonnés. L'administrateur réseau peut faire de même s'agissant de l'adressage privé qu'il met en œuvre. Or il faut souligner que ces acteurs du réseau pourraient ne pas conserver de traces de cette attribution d'une adresse, telle l'enveloppe d'une lettre qui peut être déchirée une fois la communication achevée. C'est le législateur qui est venu imposer une telle obligation de conservation en vue de pouvoir identifier tout internaute connecté au réseau.

283. **La problématique de la législation visant les données relatives au trafic.** A la fin des années 90, la législation européenne encadrant les communications électroniques vient en effet fondre le secret des correspondances dans un droit à la confidentialité des communications qui vise non plus seulement le contenu des communications mais également « *les données relatives au trafic y afférentes* »[574]. En 2002, dans le cadre de l'adoption du

[574] Dir. 97/66/CE *concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des télécommunications*, article 5, JOCE 30.1.98, L24/1-8. Il est encore toutefois fait mention du « secret des correspondances » aux cons. 2 et 17. Cette directive est abrogée dans le cadre de la création du « Paquet Télécom » par la directive 2002/58/CE dite « *vie privée et communications électroniques* »[574] qui en reprend les définitions et les principes et les développe. V. Directive 97/66/CE, JOCE 30.1.98 L24/8.

Paquet Télécom, la directive dite « *vie privée et communication électronique* »[575] consacre un principe d'effacement de telles données une fois la communication achevée. Toutefois un régime dérogatoire visant à sauvegarder « *la sécurité nationale* » est prévu qui permet par exception la conservation de certaines catégories de données relatives au trafic[576].

Une évolution qu'il faut saluer alors que le propre de la communication numérique est d'être génératrice de données qui révèlent autant que le contenu échangé et qu'il convient de protéger**.** Toutefois alors que le mouvement d'évolution du secret aurait gagné à marquer un temps d'arrêt en venant catégoriser davantage ce nouvel objet –les données produites par la communication- en prenant en considération les intérêts de la personne à protéger, le choix est fait d'adopter une définition large des données produites par la mise en œuvre d'une communication sur le réseau.

En 1997 la directive sectorielle était accompagnée d'une annexe listant les données pouvant être nécessaires à la facturation, notamment : le numéro ou le poste de l'abonné, le numéro de l'abonné appelé, la date, l'heure et la durée des appels[577]. En 2002, la directive se refuse à les définir spécifiquement[578]. L'article 2 de la directive 2002/58/CE[579] définit ainsi les données relatives au trafic comme « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation*»[580]. Or si l'on comprend qu'à l'heure de la communication numérique il ne peut s'agir d'énumérer les données produites par la communication sur le réseau alors qu'elles sont diverses et se multiplient au gré de l'acheminement du message, il est tout autant inefficace de les définir par leur seule afférence à la transmission du message.

---

[575] Dir. 2002/58/CE concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques, JOCE 31.7.2002, L201/37-43

[576] Ce régime dérogatoire fait l'objet d'une harmonisation en 2006 alors qu'est adoptée la directive 2006/ 24/CE sur la « conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications ». V. : Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE. Cette directive sera invalidée par la CJUE, dans sa décision du 8 avril 2014.

[577] Directive 97/66/CE, JOCE 30.1.98 L24/8 « Annexe » « Liste des données ». : « *Aux fins de l'article 6 paragraphe 2, peuvent être traitées les données visées ci-après indiquant : -le numéro ou le poste de l'abonné, -l'adresse de l'abonné et le type de poste, -le nombre total d'unités à facturer pour la période de facturation, le numéro de l'abonné appelé, -le type d'appels, l'heure à laquelle ils ont commencé et la durée des appels effectués et/ou la quantité de données transmises, -la date de l'appel ou du service, -d'autres informations relatives aux paiements, telles que celles qui concernent le paiement anticipé, le paiement échelonné, la déconnexion et les rappels* ».

[578] Dans son considérant n° 15, elle énonce qu'« *une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication ». Elle poursuit en donnant des exemples de données relatives au trafic qui « peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, la fin ou la durée d'une connexion. Elle peuvent également représenter le format dans lequel la communication a été acheminée par le réseau* ».

[579]V. également l'article L32-18° du CPCE

[580] *Ibid.*, article 2 «Définitions», b).

284. **Plan.** Ainsi la création d'une catégorie générale de données qui est donc nécessairement un concept est très maladroite. L'objet à encadrer devient l'objectif de la protection qui n'est plus guidée par des objectifs fondamentaux. Le but d'identification de l'internaute connecté au réseau est très imparfaitement réalisé par la législation actuelle. L'article L34-1 du CPCE fait apparaître une malfaçon **(§1).** Il convient ainsi de s'extraire de la logique d'un régime visant des données en définissant une obligation générale de localisation des points d'accès au réseau qui prend en compte la réalité physique de celui-ci pour organiser l'identification de l'internaute connecté **(§2)**

§1) La malfaçon de l'article L34-1 du CPCE

285. **La malfaçon de l'article L34-1.** En France, dès 2001, la loi pour la sécurité quotidienne introduit un article L32-3-1, désormais numéroté, L34-1, dans le code « *des postes et télécommunications* » qui enjoint les opérateurs de communications électroniques à effacer toute donnée relative à une communication une fois celle-ci achevée[581].

Toutefois par exception il est précisé qu'il peut être différé à cet effacement s'agissant de certaines catégories de données : celles qui permettent « *l'identification des personnes utilisatrices des services fournis par les opérateurs* » et celles qui ont trait aux « *caractéristiques techniques des communications assurées par ces derniers* », mais en aucun cas celles qui révèlent le contenu de la correspondance échangée[582]. En 2006 un décret vient détailler les données à conserver au premier rang desquelles figurent « *les informations permettant d'identifier l'utilisateur* »[583].

Ainsi il apparaît que l'article L34-1 énonce deux principes. D'une part il faut effacer toutes les données afférentes à la communication qui de fait dans le cadre d'une communication numérique, révèlent notamment les informations consultées via les adresses IP des sites visités. D'autre part il faut imposer la conservation d'une trace de l'attribution d'une adresse IP à un point d'accès pour permettre une investigation efficace s'agissant de l'internaute à l'origine de la connexion.

286. ***Plan.*** L'article L34-1 du CPCE vise tout à la fois le secret des informations consultées par l'internaute et la nécessaire identification de celui-ci. Le régime dérogatoire de

[581] Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, article 29. Avec la loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, le code devient le « code des postes et des communications électroniques » et la numérotation change ; cet article L32-3-1 devient l'article L34-1.

[582] Article L32-3-1, IV, alinéas 1 et 2.

[583] Décret n°2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques. Il introduit dans la partie règlementaire du CPCE un article R10-13, qui prescrit la conservation de telles données dans son I. a). Ce décret introduit également les articles R10-12 et R10-14.

conservation de certaines catégories de données, par exception au principe d'effacement, s'apparente en réalité à un principe **(A)**. Dès lors le champ d'application de cet article apparaît très incertain alors que l'identification de l'internaute doit répondre d'un régime qui lui est propre, qui n'est celui pas celui du secret des correspondances prolongé dans celui de la navigation mais qui ressort bien des conditions du contrôle de l'identité de l'internaute **(B)**.

A] Un principe de conservation par exception

287. ***Plan.*** L'article L34-1 du CPCE est créé en 2001 dans le cadre de l'adoption de la loi relative à la sécurité quotidienne, dans un chapitre mettant en œuvre des « *dispositions relatives à la lutte contre le terrorisme* »[584]. Il introduit dans le CPCE une section intitulée « *Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques* »[585].

L'objectif de cet article est d'organiser un régime d'interceptions légales de certaines catégories de données relatives au trafic. Celui-ci apparaît toutefois inadéquat alors qu'une adresse IP ne révèle rien en soi **(1)**. De fait le décret n° 2006-358 du 24 mars 2006 précisant les données de communications électroniques à conserver est inefficient s'agissant des données visant l'identification de l'utilisateur du service de communication **(2).**

1) L'inadéquation d'un régime d'interceptions légales

288. **Le principe de conservation « par exception » de certaines catégories de données techniques**. L'article L34-1 III. énonce « *qu'il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques* »[586]. L'article précise dans un dernier paragraphe que ces données « *portent exclusivement sur l'identification des personne utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques de communication assurées par ces derniers et sur la localisation des équipements terminaux.*»[587].

Dès lors la difficulté apparaît alors que l'interception ne semble donc pas viser un contenu mais renvoie à la possibilité que doivent avoir les pouvoirs publics d'identifier et de géolocaliser l'internaute connecté au réseau. De fait son articulation est illogique. Il ne s'agit pas de faire exception à la confidentialité des communications en conservant

[584] V. l'article 29 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne qui insère un nouvel article L32-3-1 dans le code des postes et des télécommunications. En 2004, le code devient le code des postes et des communications électroniques, et l'article devient le L34-1 selon la nouvelle numérotation.

[585] V. Section 3 du Chapitre II « Régime juridique », du Titre 1er « Dispositions générales », du Livre II « Les communications électroniques » du CPCE

[586] L.34-1, III, CPCE.

[587] L34-1, VI, CPCE.

des données techniques, dont il est précisé qu'elles ne peuvent porter sur le contenu des communications échangées ; il s'agit de mettre en œuvre le contrôle de l'identité de l'internaute en collectant des données permettant l'identification de celui-ci.

En réalité l'article L34-1 énonce deux principes. Toutefois cette logique, qui n'est pas celle d'un principe et d'une exception mais bien de deux principes distincts, n'apparait pas clairement dans la législation car la double fonction de l'adresse IP n'est pas distinguée.

289. **La nécessaire dissociation du régime du secret de la navigation et de celui de l'identification de l'internaute.** Pour qu'une communication s'établisse sur le réseau il faut l'adresser tout comme un courrier papier. Deux adresses sont nécessaires : l'adresse de l'expéditeur de la demande et l'adresse du site demandé. La requête de l'internaute est constituée de l'adresse du site qu'il a demandé ; le site web visualise l'adresse du point de connexion qui se connecte à lui pour pouvoir lui transmettre les informations demandées[588].

Ainsi dès qu'un utilisateur se connecte à l'internet, une adresse IP lui est attribuée mais toutes les pages du web ont également une adresse IP. Cette adresse obéit toutefois à une logique différente dès lors qu'elle est pérenne dans le temps et qu'il lui a été attribué un nom de domaine. Il apparaît alors que le relevé par le FAI au point d'accès au réseau des adresses IP demandées révèle les noms de domaines des sites visités lors de la connexion. En revanche l'adresse attribuée à la connexion n'indique rien en elle-même et s'il faut la conserver c'est dans le but de permettre la mise en œuvre d'une investigation permettant de découvrir l'identité de l'internaute connecté.

Dans son dernier paragraphe l'article L34-1 affirme dans un premier temps que les données conservées par exception le sont en vue d'identifier et de géolocaliser l'internaute, puis il est précisé qu' : « *Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications* »[589]. La formulation même de cette précision qui semble intervenir à rebours du principe est révélatrice de la malfaçon du régime opéré.

Il faut distinguer d'une part les données qui révèlent la navigation de l'internaute, des données qui adressent sa connexion. Les adresses IP des sites visités qui révèlent la

[588] Ainsi « chaque paquet de données transmis par le protocole internet (paquet IP) est étiqueté avec deux adresses IP pour identifier l'expéditeur et le destinataire. Le réseau utilise l'adresse de destination pour transmettre la donnée. Le destinataire sait à qui répondre grâce à l'adresse IP de l'expéditeur. » V. l'entrée « adresse IP », in le « Glossaire multimédia », disponible sur le site www.futura-sicences.net.

[589] L34-1, VI, CPCE.

navigation de l'internaute le temps de sa connexion sont soumises à un régime de secret qui consiste en l'obligation de les effacer une fois la connexion achevée[590]. L'adresse IP attribuée le temps de la connexion qui navigue sur le réseau doit pouvoir permettre une investigation s'agissant de l'internaute connecté et pour ce faire une concordance doit pouvoir s'opérer entre celle-ci et la localisation d'une boucle d'accès au réseau.

2) Le caractère inefficient du décret d'application n° 2006-358

290. **Le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques.** Le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques introduit trois articles, R1à-12, R10-13 et R10-14, dans la partie règlementaire du CPCE qui forment le pendant de la section nouvellement créée dans la partie législative s'intitulant « *Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques* »[591].

Il est d'abord rappelé que les données ne peuvent être collectées qu'au regard des finalités poursuivies par la loi et qu'elles doivent être « *pertinentes* » à cet égard. L'article R10-13 énonce ensuite dans son I : « *En application du II de l'article L34-1, les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales : a) Les informations permettant d'identifier l'utilisateur ; b) Les données relatives aux équipements terminaux de communications utilisés ; c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; d) Les données relatives aux services complémentaires utilisés et leurs fournisseurs ; e) Les données permettant d'identifier le ou les destinataires de la communication* ».

Ainsi l'adresse IP attribuée le temps de la connexion au réseau renvoie au : « *b), les données relatives aux équipements terminaux de la connexion utilisés* ». Par ailleurs les données visées au c), d) et e) font clairement apparaître la logique de la surveillance des communications, en permettant le comptage de celles-ci, le relevé des applications utilisées pour communiquer et celui des destinataires joints. En revanche le a) visant les « *informations permettant d'identifier l'utilisateur* » apparaît inefficient.

[590] V. *infra,* Titre II, Chapitre 2ème : « *Les conditions du suivi de la navigation d'un internaute* ».

[591] Décret n°2006-358 du 24 mars 2006, relatif à la conservation des données de communications électroniques, JORF du 26 mars 2006, Texte 9 sur 72.

291. **L'inefficience d'une obligation de conservation de données visant des « *informations permettant d'identifier l'utilisateur* » d'un service de communications électroniques**. En effet la mention du seul objectif d'identification de l'internaute ne peut systématiser les données à conserver. Par ailleurs un détail exhaustif n'est pas non plus envisageable. Enfin il est difficile de considérer dans quelle mesure ces données sont des données relatives au trafic c'est-à-dire produites automatiquement par la mise en œuvre d'une connexion. Cette obligation n'a de fait pas de sens et aboutit à des affirmations spécieuses, voire dangereuses.

Ainsi peut-t-on lire sur le site de la CNIL en 2010, dans une fiche relative à la conservation des données relatives au trafic, cette réponse à la question « *Existe-il une obligation d'identifier l'utilisateur de l'ordinateur* » : « *Non le cybercafé en question n'est pas obligé de relever et de conserver l'identité de ses clients pour fournir une connexion (ex : accès wifi ouvert). Il doit uniquement conserver les données techniques de connexion. En revanche s'il fait le choix de procéder à l'identification préalable des utilisateurs, en leur faisant remplir une fiche d'inscription par exemple, il a l'obligation de conserver ces données pendant un an* »[592]. Ce raisonnement ne tient pas. Si le titulaire de l'abonnement est libre de collecter des informations sur l'utilisateur à qui il fournit un accès, il est nécessairement libre de leur conservation. Et il faut rappeler que si quelqu'un qui met à disposition son accès peut s'enquérir de l'identité de l'individu, la liberté d'accès s'oppose à la requête de documents d'identité.

Ainsi l'obligation doit viser la localisation de la boucle d'accès au réseau mondial à laquelle a été attribuée l'adresse IP. Le régime de conservation n'a de sens que s'agissant de l'action d'adressage du réseau qui met en œuvre des données qui n'ont pas vocation techniquement à être conservées une fois la communication achevée.

B] Le champ d'application incertain de cette obligation

292. ***Plan***. Alors que la rédaction de l'article L34-1 tendait à l'origine à systématiser l'encadrement des données produites par la communication, ses modifications successives font apparaître que cet effort a échoué alors que d'une part il énumère aujourd'hui de façon inappropriée les finalités de conservation de telles données **(1)** et qu'il ne réussit pas à définir une catégorie d'acteurs du réseau soumis à une telle obligation **(2).**

[592] Site de la CNIL : cnil.fr, dans son architecture au 28 septembre 2010, rubrique « en savoir plus », « fiches pratiques », une fiche intitulée « Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ? ».

1) L'énumération inappropriée des finalités de conservation de telles données

293. **Les conditions de la conservation de ces données techniques**. Dans sa version originelle issue de la loi du 15 novembre 2001 relative à la sécurité quotidienne, le paragraphe II de l'article L34-1 s'ouvre en ces termes : « *Pour les seuls besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou rendre anonymes certaines catégories de données techniques*». C'est seulement dans le VI, le dernier paragraphe de l'article, qu'il est précisé que ces données conservées et traitées « *portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques de communication assurées par ces derniers et sur la localisation des équipements terminaux* ».

Or cette rédaction fait apparaître un illogisme dans les prescriptions mises en œuvre. En effet ce n'est pas l'objectif d'identification de l'internaute qui fonde la conservation des données alors qu'il n'apparaît que dans un second temps et à côté de l'objectif de géolocalisation de l'internaute. Tel que l'article est rédigé ce qui fonde la conservation des données est en réalité la nécessité de les conserver ; puisqu'il faut pouvoir les mettre à disposition de l'autorité judiciaire dans le cadre d'une instance pénale.

Ainsi un glissement s'opère entre le fondement de l'obligation de conservation des données et les conditions de l'accès à de telles données comme en témoigne l'évolution de la rédaction de cette première phrase du paragraphe II qui ne va cesser de s'allonger au cours des années. En 2009 l'article est ainsi complété par la loi dite « HADOPI I»[593] : les données sont conservées pour les besoins de la recherche, de la constatation et de la poursuite non plus seulement des infractions pénales mais également quand il s'agit d'établir « *un manquement à l'obligation définie à l'article L336-3 du code de la propriété intellectuelle* ». Dès lors le but de la conservation des données n'est plus celui de les mettre à disposition de la seule l'autorité judiciaire ; elles doivent être également accessibles à « *la haute autorité mentionnée à l'article L331-12 du code de la propriété intellectuelle* ». Enfin la loi **relative à la programmation**

[593] V. article 14, Loi n°2009-669 du 12 juin 2009 relative à favorisant la diffusion et la protection de la création sur internet.

militaire de décembre 2013[594] ajoute que les données sont conservées pour « *les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal* » et qu'elles doivent être mises à disposition de « *l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense*. ».

Le paragraphe II de l'article L34-1 énonce en réalité les conditions du contrôle de l'identité de l'internaute qui ne peut être le fait que du pouvoir régalien, que ce soit le juge judiciaire dans le cadre d'une instance pénale ou une autorité administrative qui y est habilitée par la loi[595].

2) La définition ineffective des acteurs soumis à l'obligation de conservation

294. **La rédaction originelle de l'article L34-1.** A l'origine l'article L34-1 ne vise que « *les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communications en ligne* ». Ainsi dans une logique de confidentialité des communications et d'interceptions de certaines données sont d'abord visés les acteurs qui mettent en œuvre structurellement la connexion au réseau[596]. Sont visés plus particulièrement parmi ces opérateurs de communications électroniques, les FAI qui sont en lien direct avec des abonnés ; les données qu'ils traitent révèlent en effet dès lors des informations personnelles.

Toutefois cette définition des FAI qui emploie une formulation générale peut prêter à confusion. Ainsi en 2005, la Cour d'Appel de Paris qualifie la société BNP Paribas de prestataire technique « *dont l'activité est d'offrir un accès à des services de communications en ligne »*[597]. La société est ainsi tenue de fournir toute information de nature à permettre l'identification de l'auteur d'un courriel litigieux. En effet, si l'exégèse de l'article est claire au regard du droit des communications électroniques qui définit le prestataire technique en considération de son accès à l'infrastructure du réseau mondial et de la mise en œuvre dès lors d'un réseau ouvert au public[598], sa rédaction

[594] V. article 24, Loi **n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF du 19 déc. 2013, texte 1 sur 163.**

[595] V. *infra Section II* « Les conditions de divulgation du point d'accès au réseau associé à l'adresse IP».

[596] V. l'article L32, 15°, CPCE.

[597] CA Paris, 14ème ch. sect.B., arrêt du 4 février 2005, S.A. BNP PARIBAS c/ Société WORLD PRESS ONLINE. V. l'article de BOUBEKEUR Iliana, « Une entreprise peut se voir attribuer la qualité de fournisseur d'accès à l'Internet », article mis en ligne sur le site juriscom.net, le 04/04/2005.

[598] V. la définition du « réseau ouvert au public » à l'article L32, 3° du CPCE, à opposer aux définitions du réseau indépendant et celle du réseau interne, v. l'article L32, 4° et 5° du CPCE. Le réseau ouvert au public met en œuvre des services dont l'usage est ouvert à tous ; l'infrastructure qui le réalise appartient au domaine public.

suscite des questions. Des incertitudes se font jour s'agissant du champ d'application de l'obligation de conservation de données prévues à l'article L34-1 alors que par ailleurs, mis à part l'accès possible au réseau à partir du poste de son entreprise, d'autres modes d'accès au réseau commencent à se développer au milieu des années 2000.

295. **L'ajout d'un nouvel alinéa en 2006 par la loi de lutte contre le terrorisme**. Ainsi face à l'évolution des modes d'accès au réseau alors que les cybercafés et les points d'accès en wifi se multiplient, le législateur ajoute en 2006 dans le cadre d'une loi visant la lutte contre le terrorisme un nouvel alinéa à l'article L34-1[599]. Désormais sont également astreintes à l'obligation d'effacement des données relatives au trafic et par exception donc à la conservation de certaines d'entre elles : « *les personnes qui, au titre d'une activité principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit* »[600].

Si un effort de conceptualisation peut être noté alors que la logique de l'accès au réseau mondial via un sous-réseau est prise en compte, le champ d'application de ce nouvel alinéa n'en est pas moins restreint. En effet, il vise l'accès au réseau mis à disposition dans le cadre d'une relation commerciale, que l'accès au réseau soit l'objet de cette relation ou qu'il soit envisagé comme un service délivré en sus de la prestation principale[601]. Dès lors la problématique demeure de savoir ce qu'il en est d'une catégorie importante de sous-réseaux qui ne s'inscrivent pas dans un tel rapport comme ceux d'une entreprise, d'une université ou d'une administration.

La CNIL dans son avis relatif au projet de loi, avait souhaité que les catégories de personnes morales ou physiques visées par ce nouvel alinéa soient précisées ; à défaut elle convient alors que les entreprises et les administrations ne sont pas visées par ce nouvel alinéa[602]. Toutefois cette affirmation est encore questionnée en 2011 alors que l'article est modifié pour acter de la révision du Paquet Télécom.

296. **La rédaction d'un nouveau paragraphe introductif à la suite de la révision du Paquet télécom.** L'ordonnance n°2011-1012 du 24 Août 2011 relative aux communications

[599] V. article 5, loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

[600] Article L34-1, II, alinéa 3, CPCE.

[601] Ainsi l'exposé des motifs de la loi 2006-64 énonce qu'il faut encadrer les connexions « également possible à partir de lieux publics ou commerciaux, via des bornes d'accès sans fil (WIFI), ou par l'intermédiaire d'un réseau distribué, communément appelé « cybercafé », V. le dossier législatif disponible sur le site de l'Assemblée Nationale, assemblée-nationale.fr

[602] V. Délibération n°2005-208 du 10 octobre 2005 portant avis sur le projet de loi relatif à la lutte contre le terrorisme, disponible en ligne sur le site de la CNIL.

électroniques qui transpose les directives de 2009 révisant le Paquet Télécom[603] introduit un nouveau paragraphe initial à l'article L34-1 du CPCE : « *Le présent article s'applique au traitement de données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge des dispositifs de collecte et d'identification* ».

Ce nouveau paragraphe introductif ne modifie pas le régime des obligations relatives aux données relatives au trafic et n'élargit pas les acteurs qui y sont soumis. Il acte en réalité de la dilution de principe de confidentialité des communications dans un mécanisme de sécurisation des données collectées alors que de nouveaux procédés de collecte apparaissent, comme les puces RFID, qui communiquent et transmettent des informations[604]. Le législateur européen a précisé que les dispositions adoptées portent « *sur les réseaux et services de communications électroniques publics et ne s'applique pas à des groupes fermés d'utilisateur ou à des réseaux d'entreprise* »[605].

Toutefois la rédaction adoptée par la généralisation qu'elle opère peut prêter à confusion et certains s'interrogent à nouveau sur l'inclusion des réseaux d'entreprise[606]. En effet, il est difficile de considérer que les sous-réseaux des collectivités n'aient pas à répondre des adresses IP qu'ils attribuent à leurs points d'accès. Cependant, de la même manière, il est difficile de les inclure dans un régime qui vise en premier lieu la confidentialité des communications alors que ces réseaux sont fondés à surveiller les choix de connexions de leurs salariés s'ils les ont informés du traitement de données opéré[607]. En distinguant le régime du secret de la navigation de celui de l'identification de l'internaute, il peut être formulé une obligation générale. Toute personne qui met à disposition un accès au réseau doit pouvoir répondre des données d'adressage de celui-ci.

[603] V. les deux directives du Parlement européen et du Conseil du 25 novembre 2009, la directive 2009/140/CE modifiant la directive CADRE, la directive ACCES et la directive AUTORISATION , et la directive 2009/136/CE du 25 novembre 2009 du Parlement européen et du Conseil modifiant la directive SERVICE UNIVERSEL et la directive VIE PRIVEE ET COMMUNICATION.

[604] V. cons. 56, directive 2009/136/CE. V. également : CHASSIGNEUX C. « Regards sur la violation de données à caractère personnel », *CCE* n°12, Décembre 2011, étude 23.

[605] V. cons. 55, directive 2009/136/CE.

[606] V. CAPRIOLI E., « Notification des violation de données à caractère personnel », *CCE* 2011, comm.116.

[607] V. : G.CRIQUI-BARTHALAIS, « " les connexions établies par un salarié sont présumées avoir un caractère professionnel"» Arrêt de la chambre sociale de la Cour de Cassation du 9 juillet 2008 », article initialement mis en ligne en 2008 sur le site du CEJEM, cejem.com, actuellement indisponible. V. *infra :* Titre II, Chapitre 2ème, Section II : « *Le régime du secret de la navigation de l'internaute* ».

§2) La définition d'une obligation générale de localisation des points d'accès au réseau

297. **La formulation d'une obligation nouvelle.** Il a été montré que le point de départ d'une investigation efficace s'agissant de l'identification de l'internaute connecté n'était pas les coordonnées de l'abonné qui pouvait être une personne morale mais la localisation du point d'accès au réseau utilisé qui correspond toujours à un périmètre de connexion restreint. Une obligation nouvelle s'agissant des données d'adressage peut ainsi être rédigée : toute personne qui attribue une adresse IP, qu'elle soit publique ou privée, à une machine doit répondre de cette action. Ainsi il faut d'abord considérer le champ d'application d'une telle obligation de conservation des adresses IP attribuées au point d'accès **(A)**. Il conviendra ensuite d'envisager son régime **(B).**

A] Le champ d'application de cette obligation

298. **Une systématisation efficace**. La logique de l'adressage du réseau a été détaillée dans le titre premier qui traitait de la fonction de l'adresse IP attribuée à chaque connexion. Il a été expliqué que deux niveaux d'adressages peuvent être mis en œuvre sur le réseau : un adressage dit public à l'échelle du réseau mondial, et un adressage dit privé à l'échelle de sous-réseaux étendus pouvant être mis en œuvre à partir d'un point d'accès au réseau mondial. L'adressage public est le fait des opérateurs de communications électroniques ; l'adressage privé est le fait d'un administrateur-réseau. De fait ces deux acteurs intervenant dans l'adressage du réseau doivent être visés par l'obligation de conserver toute trace de l'attribution d'une adresse IP, qu'elle soit publique ou privée à un point de connexion au réseau.

L'obligation doit ainsi consister en la conservation d'une trace de l'action d'adressage. A l'échelle de l'opérateur de communications électroniques et de l'administrateur-réseau, il doit y avoir un fichage des adresses IP, en ce sens que toute adresse IP circulant sur le réseau doit pouvoir être associée au point d'accès au réseau auquel elle a été attribuée. Un traitement de données doit être mis en œuvre qui permet une concordance entre une adresse IP relevée sur le réseau et la localisation du point d'accès qui l'a émise.

299. **Le fichage des points d'accès et non la collecte d'informations visant l'internaute**. Il faut souligner que quand bien même dans le cadre d'un réseau mis à disposition du public ou d'un sous-réseau administré des informations pourraient être recueillies sur l'internaute

pour l'identifier ou pour authentifier sa connexion par le titulaire de la ligne, ces formulaires ou droits d'accès sont mis en œuvre librement par l'abonné au réseau.

Si de telles données sont collectées, la logique n'est pas d'envisager un régime de conservation mais bien de secret puisqu'il ne peut s'agir que tout quidam puisse obtenir de telles informations d'un opérateur ou de l'administrateur d'un réseau local. Il faut dès lors réfléchir aux conditions de la levée d'un tel secret. De fait dans le cadre d'une instance pénale visant la révélation du point d'accès utilisé, elles seront nécessairement mises à disposition de l'autorité judiciaire.

Ainsi ce qui importe est de mettre en œuvre un régime légal de conservation de données techniques qui permette de pouvoir considérer le terminal du réseau local à partir duquel la connexion a été opérée. Une investigation pourra alors être mise en œuvre qui seule pourra attester qu'un individu est à l'origine d'une connexion litigieuse en prouvant sa présence physique derrière la machine servant de point d'accès ou à proximité de celle-ci dans le cas d'un accès au réseau mis en œuvre par un signal wifi.

B] Le régime de cette obligation

300. **Une durée de conservation limitée**. Cette conservation de données doit être limitée dans le temps alors que doit être respecté la liberté d'accès au réseau et que par ailleurs la volatilité des connexions sur le réseau et donc des adresses IP circulant sur celui-ci rend une conservation longue inutile. En ce sens le délai de 1an à compter du jour de l'enregistrement du décret n°2006-358 du 24 mars 2006 pris en application de l'article L34-1 du CPCE peut être repris s'agissant de cette obligation générale de fichage des adresses IP au regard des points d'accès utilisés[608].

La logique est ici celle de la réactivité face à une connexion suspecte. L'identification de l'internaute connecté au réseau renvoie à sa liberté d'accès. L'internaute s'engage dès lors qu'il se connecte au réseau via une adresse IP valide. Son adresse IP circule sur le réseau et elle peut être enregistrée à l'autre bout de la communication en vue de son identification. Toutefois la possibilité qu'il puisse être identifié à partir de cette adresse doit opérer un équilibre entre sa liberté d'accès qui serait méconnue si toutes ses connexions pouvaient être indéfiniment enregistrées et la nécessité qu'il puisse répondre de ses actes. En réalité, la requête visant l'accès aux données permettant de localiser le point d'accès utilisé vise une action immédiate face à une infraction constatée.

[608] Décret n°2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques

La problématique peut être plus délicate à l'endroit de la mise en ligne d'un contenu litigieux qui perdure dans le temps[609]. Or on soulignera que, au-delà de ce délai de conservation de 1 an qui limite la possibilité de connaître le point d'accès utilisé et l'identité de l'internaute connecté, un contenu litigieux peut toujours être retiré après notification s'il s'avère illicite. Par ailleurs la législation veille à ce qu'une interaction avec l'auteur de la mise en ligne soit rendue possible.

301. **La compensation des surcoûts liés à la mise en œuvre d'un tel traitement**. Par ailleurs il faut préciser que les surcoûts identifiables et spécifiques supportés par l'opérateur pour conserver une trace de la répartition des adresses IP entre les points d'accès qu'ils mettent à disposition doivent être compensés[610]. En effet le Conseil constitutionnel a jugé que « *S'il était loisible au législateur, dans le respect des libertés constitutionnellement garanties d'imposer aux opérateurs de réseaux de télécommunications de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt général de la population est étranger à l'exploitation des réseaux de télécommunications, que les dépenses en résultant ne sauraient dès lors en raison de leur nature, incomber directement aux opérateurs »*[611]. Ce raisonnement peut être repris pour les opérateurs de communications électroniques déclarés à l'ARCEP qui n'ont pas à répondre de la mise à disposition des points d'accès relevant du domaine public.

Il ne peut en aller de même s'agissant de la conservation des adresses IP dans le cadre de la mise en œuvre de sous-réseaux locaux. En effet dans ce cas, l'entité qui met en œuvre ce sous-réseau s'il ne veut pas répondre des connexions mises en œuvre sur celui-ci doit supporter la conservation des données permettant une investigation efficace s'agissant de la localisation du point d'accès à l'origine de la connexion. Elle doit être à même de considérer tout point d'accès utilisé au regard d'un numéro IP privé qui lui a été attribué. A défaut elle engage sa responsabilité.

---

[609]. V. pour une affaire où un éditeur de presse agit en contrefaçon de contenus et obtient sur requête judiciaire de l'hébergeur, les adresses IP à l'origine de la mise en ligne mais tarde toutefois à saisir le juge pour obtenir les coordonnées de l'abonné et du point d'accès utilisé auprès des FAI, ce qui fait que le délai de 1an étant passé, celles-ci ont été légalement effacées : CA, Paris, 3ème ch. , 15 déc. 2015, *ETAI* c/*SFR, Manche Télécom, RLDI* 2015, n°1595.

[610] V. l'introduction par le décret n°2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques d'un article R10-13- dans le CPCE, qui renvoie à l'article R213-1 du Code de procédure pénale et à l'arrêté 21 août 2013 pris en application des articles R. 213-1 et R. 213-2 du code de procédure pénale fixant la tarification applicable aux réquisitions des opérateurs de communications électroniques.

Par exemple il est arrêté ce coût : « A partir d'une demande dématérialisée conforme sur des adresses IP horodatées, rechercher sommairement dans le SI le plus pertinent les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques. De 1 à 20 : 4 € Au-dessus de 20 : 0,18 € par IP »

[611] Décision 2000-441 DC du 28 décembre 2000, loi de finance rectificative pour l'année 2000. *D.* 2001, somm. P. 1842, obs. D.Ribes.

Conclusion du chapitre 2ème

302. **Le régime de l'identification de l'internaute connecté au réseau : deux principes**. Ce régime répond d'une interdiction et d'une obligation.

D'une part il faut interdire tout système d'identification de l'internaute qui n'a pas à être identifié pour se connecter. L'adresse IP ne permet aucune identification automatique de l'internaute connecté. Elle renvoie simplement à un point de connexion connu de la personne qui a attribué l'adresse à ce terminal d'accès. Ainsi il faut garantir le respect du mécanisme d'adressage du réseau qui ne permet pas une identification automatique de l'internaute connecté à partir de l'adresse IP visible sur le réseau. Il faut également interdire aux pouvoirs publics de requérir de l'internaute qui souhaite se connecter au réseau qu'il décline son identité civile. Le respect de la liberté d'accès au réseau impose qu'une investigation soit nécessaire pour considérer celle-ci. Or il convient de permettre cette investigation.

Ainsi, d'autre part, il faut organiser le fichage des points d'accès au réseau. En effet la logique de l'attribution d'une adresse IP répond d'une logique d'immédiateté : à une connexion opérée à un instant « t » est attribuée une adresse IP pour que les informations demandées lui parviennent. Toutefois, une fois la communication terminée, cette adresse IP n'a plus d'utilité et peut même être attribuée à un autre point d'accès. Apparaît la nécessité de pouvoir considérer rétroactivement l'action d'adressage afin de localiser le point d'accès utilisé et de découvrir qui y était connecté.

303. **La définition d'une obligation nouvelle de localisation des points d'accès**. A cet endroit le régime actuel de l'article L34-1 du CPCE fait apparaître une malfaçon alors que visant généralement les données relatives au trafic, c'est-à-dire produites par toute connexion au réseau, il ne permet pas d'appréhender clairement et concrètement le régime devant permettre l'identification de l'internaute connecté. Une obligation nouvelle doit être définie qui doit viser de manière générale l'action d'adressage en vue de permettre cette identification.

Ainsi il doit être affirmé que toute personne qui attribue à un point d'accès une adresse IP doit être à même de répondre de cette action ; et ce, que l'adresse soit publique ou privée comme dans le cas d'un réseau local mis en œuvre par un administrateur-réseau. Toute adresse IP visible sur le réseau doit pouvoir conduire à la

dernière boucle du réseau qui l'a mise en œuvre ce qui délimite un espace de connexion restreint. Ainsi toute adresse IP renvoie non pas à un individu mais bien à un lieu défini ce qui ménage la liberté d'accès de l'internaute tout en organisant un fichage qui permette de le retrouver pour qu'il puisse répondre de ses actes.

CONCLUSION DU TITRE I.

304. **Le respect de l'anonymat sur le réseau.** Le titre I a montré que le mécanisme d'adressage du réseau permet l'anonymat de l'internaute. L'identité d'un internaute peut être considérée grâce à son adresse IP mais ne l'est jamais automatiquement. La mise en œuvre d'un régime légal de fichage des points d'accès au regard des adresses IP qu'ils émettent et qui circulent sur le web permet à l'internaute connecté d'être retrouvé via cette adresse mais cela nécessite une investigation et donc des moyens humains.

Ainsi cet anonymat fonde la liberté d'accès au réseau et de navigation sur la toile de tout internaute puisqu'en aucun cas ses faits et gestes ne peuvent être reliés automatiquement à son identité civile. Toutefois en vue d'assurer le respect de l'ordre public, une fois connecté, l'internaute peut être soumis à une surveillance, qui doit être régulière, c'est-à-dire qu'elle doit opérer une conciliation entre les intérêts supérieurs de la nation et notamment l'exigence de sécurité pour tous et le respect des libertés individuelles de chacun.

TITRE II. LES LIMITES A LA SURVEILLANCE DE L'INTERNAUTE NAVIGUANT SUR LE WEB

305. **Les limites de la surveillance de l'internaute**. Comme il a été montré l'adresse IP permet d'identifier toute personne à l'origine d'une connexion au réseau dès lors qu'est mis en œuvre un fichage des points d'accès au réseau au regard de telles adresses. Ainsi l'anonymat sur le réseau, tout comme dans le monde physique, n'est jamais total et c'est ce qui fonde la liberté d'accès et de naviguer sur le réseau : l'internaute s'engage nécessairement en agissant sur le réseau.

Toutefois pour sauvegarder ces libertés il convient de définir un régime strict permettant ce contrôle de l'identité de l'internaute. Tout comme dans le monde physique, celui-ci ne peut ressortir que du pouvoir régalien et être mis en œuvre selon une procédure définie par la loi et respectueuse des libertés fondamentales de l'individu. Par ailleurs tout internaute connecté doit avoir l'assurance que sa navigation ne fait pas l'objet d'un suivi arbitraire. Ainsi ses choix de navigation doivent être effacés une fois la connexion terminée ; par exception il faut définir les régimes permettant une filature numérique.

306. ***Plan*.** Dans un premier temps seront définies les conditions du contrôle de l'identité de l'internaute connecté au réseau **(Chapitre 1er).** Dans un second temps sera étudié le régime du suivi de la navigation de l'internaute sur le web **(Chapitre 2ème).**

Chapitre 1er. Les conditions du contrôle de l'identité de l'internaute

Chapitre 2ème. Les conditions du suivi de la navigation de l'internaute

Chapitre 1er. Les conditions du contrôle de l'identité de l'internaute

307. **Le contrôle de l'identité de l'internaute.** La logique du contrôle de l'identité de l'internaute sur le réseau s'articule en deux temps.

Il faut techniquement d'abord relever une adresse IP circulant sur le réseau. Cette opération ne semble poser aucune problématique ; cependant la qualification d'une adresse IP en tant que donnée personnelle vient semer le doute sur les conditions de la collecte d'une telle donnée. Or il faut considérer que par essence elle réalise la connexion et opère donc le lien nécessaire entre les individus communiquant entre eux. Le principe doit être la liberté de collecter une telle donnée qui en soi ne révèle rien.

C'est là qu'intervient la seconde partie du raisonnement. Il faut considérer les conditions de l'accès au fichier réalisant la concordance entre cette adresse et la localisation du point d'accès qui l'a émise. Des doutes subsistent s'agissant des conditions de la divulgation d'une telle information : de simples poursuites civiles permettent-elles celle-ci ? Il sera affirmé que non alors que le contrôle de l'identité de l'internaute ne peut ressortir que du pouvoir régalien.

308. **Plan.** Ainsi il faut s'interroger d'abord sur les conditions de la collecte d'une adresse IP circulant sur le réseau **(Section I).** Puis il faut clarifier les conditions de la divulgation du point d'accès utilisé **(Section II).**

Section I : Les principes devant guider la collecte d'une adresse IP circulant sur le réseau

309. **La mise en œuvre de différents fichiers d'adresses IP par les services du web.** Il faut considérer deux types de collectes d'adresses IP : la première vise la collecte des adresses à l'origine d'une simple connexion à un réseau local comme un intranet ou un réseau de P2P, ou d'une simple connexion à un site du web. L'objectif premier ici n'est pas l'identification de l'internaute mais la surveillance même des connexions en vue de détecter une intrusion frauduleuse ou une attaque informatique. L'enjeu est ici celui du régime de la mémorisation de telles adresses alors qu'une telle collecte peut s'apparenter à un procédé de vidéosurveillance. Autrement dit il faut considérer dans quelle mesure peut être mis en œuvre le contrôle de l'identité d'un individu visitant un site web ou se connectant à un sous-réseau.

La seconde renvoie à la collecte obligatoire des adresses IP à l'origine de la mise en ligne de contenus sur le web. Cette collecte est rendue obligatoire par l'article 6.II de la LCEN[612] alors qu'il est nécessaire de conserver ces adresses pour permettre la mise en œuvre de la responsabilité de l'internaute, qui ici n'est pas simple naviguant, mais a édité du contenu en ligne.

310. ***Plan.*** Ainsi il est proposé de réfléchir dans un premier temps au régime de la collecte de toutes les adresses IP se connectant à un réseau local ou un site web et d'opérer pour ce faire une analogie avec la vidéosurveillance **(§1)**. Il faut par ailleurs considérer l'évolution de l'obligation légale de l'article 6.II. de la LCEN visant la collecte de toute adresse IP à l'origine de la création d'un contenu **(§2)**.

§1) La liberté de collecter toute adresse IP se connectant à un site web ou à un sous-réseau

311. **L'analogie avec les procédés de vidéosurveillance.** Il est envisagé dans cette étude de considérer l'adresse IP comme le visage découvert d'un internaute. La collecte des adresses IP se connectant à un réseau local ou à un site du web pourrait alors s'apparenter à un procédé de vidéosurveillance. Or dans le monde physique ces procédés ne peuvent pas être librement mis en œuvre ; ils relèvent d'un régime d'autorisation alors que leur principe même porte atteinte à la liberté individuelle dès lors que les actions d'un individu ne peuvent pas en dehors de toute finalité précisée être enregistrées sur une bande vidéo.

Le 21 janvier 1995 une loi vient encadrer ces procédés de vidéosurveillance qui se multiplient notamment sur la voie publique[613]. L'article 1er de la loi énonce que : « *La sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives.* ». Le législateur définit ici une nouvelle liberté publique et cherche à organiser sa mise en œuvre[614]. Le Conseil constitutionnel est saisi par soixante députés et soixante sénateurs qui citent le « *Big Brother is watching you* » d'Orwell[615]. Il

[612] V. : Loi n° 2004-575 du 21 juin 2004 pour la Confiance en l'économie numérique dite loi « LCEN », J. O. du 22 juin 2004, texte 2 sur 108.

[613] V. : Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (JORF du 24 janvier 1995, p.1249) dite « Loi Pasqua ». Elle peut être considérée comme la première loi du type « LOPSI » pour « orientation et programmation de la sécurité intérieure ». V. également le décret n°96-296 du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application de l'article 10 n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

[614] Le Doyen Favoreu souligne que cet article témoigne d'une « *conception aujourd'hui dépassée » des libertés publiques « privilégiant la protection par le législateur et le juge ordinaire* ». FAVOREU L., Revue française de droit constitutionnel, n°22, 1995, p.362.

[615] Saisine du Conseil constitutionnel en date du 23 décembre 1994, présentée par plus de soixante députés, en application de l'article 61, alinéa 2, de la Constitution, et visés dans la décision n°94-352 DC, JORF du 21 janvier 1995, p.1156. Saisine du Conseil constitutionnel en date du 23 décembre 1994, présentée par plus de soixante sénateurs, en application de l'article 61, alinéa 2, de la Constitution, et visés dans la décision n°94-352 DC, JORF du 21 janvier 1995, p.1159.

énonce alors que « *la prévention des atteintes à l'ordre public, notamment d'atteintes à la sécurité des personnes et des biens, et la recherche des auteurs d'infractions sont nécessaires à la sauvegarde de principes et droits à valeur constitutionnelle* » et qu'une conciliation doit s'opérer *« entre ces objectifs à valeur constitutionnelle et l'exercice des libertés publiques constitutionnellement garanties au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir ainsi que l'inviolabilité du domicile* »[616]. Pour la première fois, il affirme que « *la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* »[617].

En l'espèce alors que les procédés de vidéosurveillance sont soumis à un régime d'autorisation qui les circonscrit et à une procédure qui contrôle leur proportionnalité au regard des objectifs visés, cette conciliation a lieu[618].

312. **Les limites de l'analogie s'agissant des traitements automatisés d'adresses IP**. Toutefois il sera montré qu'il convient à l'endroit de la collecte des adresses IP sur le réseau d'opérer une distanciation alors que ces données techniques réalisent la seule interaction entre un internaute et un service.

Cette collecte est nécessairement généralisée pour permettre le bon fonctionnement des services qui par ce biais peuvent conserver une trace des connexions mises en œuvre. La finalité d'un tel fichier est légitime alors qu'il permet de constater une intrusion frauduleuse dans un système ou de détecter une attaque informatique. Une telle conservation par des opérateurs privés ne porte par atteinte à la liberté d'accès au réseau de l'internaute alors que l'identification de celui-ci le cas échéant à partir de l'adresse IP enregistrée ne peut intervenir que dans le cas d'une procédure pénale en application de l'article L34-1 du CPCE[619].

---

[616] Décision n°94-352 DC du 18 janvier 1995. V. : sur l'article 10, le considérant n°2.

[617] *Ibid.* Ainsi la formulation de la liberté individuelle s'enrichit de l'aspect « *respect de la vie privée* » sans toutefois qu'il soit tranché sur la définition de cette liberté qui conditionne la compétence exclusive du juge judiciaire. En l'espèce s'agissant du contrôle des procédés de vidéosurveillance l'autorité judiciaire n'est sollicitée que de manière indirecte alors que la commission départementale qui doit donner son avis avant toute installation est présidée par un magistrat.

[618] Initialement encadrés par l'article 10 de la loi n°95-73 du 21 janvier 1995 (Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (JORF du 24 janvier 1995, p.1249), ce régime va s'étoffer au fil des législations de sécurité successives le régime pour être finalement codifié en 2012 dans le code de la sécurité intérieure (V. : Loi n°2006-64 du 23 LOI n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant disposition diverses relatives à la sécurité et aux contrôles aux frontières -JORF du 24 janvier 2006, p. 1129-, chapitre 1er « Dispositions relatives à la vidéosurveillance » ; Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure -JORF du 15 mars 2011, p. 4582-, chapitre 1er, section 4 « *vidéo-protection* » ; Ordonnance 2012-351 du 12 mars 2012 relative à la partie législative du Code de la Sécurité Intérieure -JORF du 13 mars 2012, texte 15 sur 112-).

Sous la dénomination adoptée depuis 2011 de « vidéo-protection », la mise en œuvre de caméras est encadrée aux articles L251-1 à L254-1 de ce code ainsi qu'aux articles L223-1 à L223-9 qui traitent spécifiquement de la mise en œuvre de tels systèmes dans le cadre de la lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la nation.

[619] V. *infra* Section II : « *La procédure permettant la divulgation du point d'accès au réseau* ».

En revanche la mise en œuvre d'une telle collecte par les services de l'État doit être encadrée spécifiquement. En effet, la collecte des adresses répond alors d'un objectif de police administrative visant la préservation de l'ordre public et la prévention des infractions. Une conciliation doit s'opérer entre ces objectifs légitimes de sécurité et la liberté d'accès de l'internaute au réseau alors que les agents spécialisés peuvent avoir accès au fichier localisant le point d'accès au réseau dans le cadre de réquisitions administratives[620]. Ainsi cette surveillance des adresses IP visibles sur le réseau qui cherche à identifier l'internaute connecté doit répondre d'un régime strict d'autorisation qui la circonscrit au regard de finalités précisées et la soumet à une procédure définie.

313. ***Plan.*** Il faudra ainsi affirmer d'une part un principe de liberté collecter toute adresse IP au profit de l'administrateur d'un réseau local ou d'un site du web **(A)** puis envisager le régime de cette même collecte d'adresses IP quand elle est à l'instigation des pouvoirs publics **(B).**

A] Le principe de cette liberté de collecte nécessaire au fonctionnement du réseau

314. **Le principe de la liberté de collecter une adresse IP attribuée à chaque connexion au réseau.** Le chapitre premier a montré l'inadéquation du champ d'application de la protection des données personnelles s'agissant de la qualification de l'adresse IP et de la collecte qui peut en être faite. Il ne s'agit pas de considérer la finalité légitime de la collecte par le responsable du traitement ou à défaut de vérifier que le consentement de l'internaute ait été requis.

Le raisonnement tenu dans l'arrêt Breyer qui différencie l'objectif légitime visant « *à garantir, au-delà de chaque utilisation concrète de leurs sites internet accessibles au public, la continuité du fonctionnement desdits sites* »[621] de l'objectif en réalité poursuivi par le site web du gouvernement allemand «*visant à garantir la capacité générale de fonctionnement* »[622] nous paraît spécieux. Un site doit pouvoir protéger l'intégrité de ses services d'une manière générale. On rappellera également les difficultés de la CNIL à considérer dans quelle mesure un site web peut conserver des adresses IP à l'origine par exemple de la création de comptes pour détecter des faux-profils et exclure l'utilisateur qui ne respecte pas les CGU du site[623]. Alors qu'apparaissent des incertitudes sur le sens de la finalité légitime pour un site web lui

[620] *Ibid.*
[621] CJUE (aff. C-583/14), 19 octobre 2016, *Patrick Breyer c/ Bundesrepublik Deutschland*.., point n°60.
[622] *Ibid.*, point n°64.
[623] V. *supra* n°247

permettant de collecter les adresses IP ou à défaut sur le sens de la requête d'un consentement de l'internaute qui nécessairement tendrait alors à se généraliser, l'autorité administrative appelle à une rationalisation de ces problématiques grâce à des normes.

En effet, il est légitime d'une manière générale qu'un site puisse se ménager la possibilité de considérer qui se connecte à lui à travers la conservation des adresses IP qui ne permettent en aucun cas d'identifier automatiquement un individu. Il doit être affirmé le principe de la liberté de la collecte de toute adresse IP se connectant à un site web, adresse qui permet non pas l'identification de l'internaute par le site web mais qui établit une nécessaire interaction avec l'individu connecté. Cette collecte ne peut ressortir du consentement de l'internaute alors qu'il est obligé à ce minima démocratique qui lui impose d'agir à visage découvert.

315. ***Plan.*** Le sens du principe de la liberté répond de la nécessité pour l'administrateur d'un réseau ou d'un site de mémoriser les adresses des connexions à son service **(1)**. L'objectif d'une telle collecte qui vise le fonctionnement même du service renvoie de fait à un délai de conservation court **(2).**

1) La mémorisation nécessaire des connexions à un réseau local ou à un site web

316. **Les interrogations quand au régime de la collecte des adresses IP se connectant à un site web.** Il faut d'emblée rappeler qu'en 1995 lorsqu'a été établi le régime des procédés de vidéosurveillance, la CNIL a critiqué que de tels procédés soient soustraits à son contrôle arguant de la nature personnelle du visage d'un individu[624]. Là n'est pas la problématique alors que les seuls traits d'un visage n'identifient pas et que les fichiers mis en œuvre dans le cadre de ces procédés ne sont jamais nominatifs[625]. Tout comme la collecte d'une adresse IP et le fichier que peut mettre en œuvre l'administrateur d'un réseau ou d'un site du web.

---

[624] CNIL, Délibération 94-056 du 21 juin 1994 **« portant adoption d'une recommandation sur les dispositifs de vidéosurveillance mis en œuvre dans les lieux publics et les lieux recevant le public ». La Commission affirme ainsi que « *lorsqu'elles sont captées par la caméra d'un système de vidéosurveillance, les images des personnes doivent être regardées comme des informations nominatives permettant, au moins indirectement, par rapprochement avec d'autres critères, l'identification de ces personnes ; qu'il en est de même notamment des plaques d'immatriculation des véhicules en cela qu'elles peuvent permettre l'identification des propriétaires ; ».**

[625] Article 10.-I., Loi n° 95-73 du 21 janvier 1995. Cet article dispose que « *Les enregistrements visuels de vidéosurveillance ne sont considérés comme des informations nominatives, au sens de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, que s'ils sont utilisés pour la constitution d'un fichier nominatif* ». La loi dite « LOPSI II » en 2011 vient toutefois préciser que *« Seuls sont autorisés par la Commission nationale de l'informatique et des libertés, en application de la loi no 78-17 du 6 janvier 1978 précitée, les systèmes installés sur la voie publique ou dans des lieux ouverts au public dont les enregistrements sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques*».

En réalité en établissant une analogie entre la collecte d'une adresse IP se connectant à un site web et la vidéosurveillance que permet une caméra installée par exemple dans un commerce, l'interrogation est de savoir si, à l'instar des procédés du monde physique, l'enregistrement d'une adresse IP doit répondre d'une finalité stricte et faire l'objet d'une autorisation ; en ce sens que par principe cet enregistrement est prohibé alors qu'il porte atteinte à la liberté individuelle de l'internaute s'il n'est pas motivé par un objectif à valeur constitutionnelle visant la sauvegarde des libertés publiques.

Dans une décision du 12 mars 2014, le Conseil d'État relève que la société « *Pages Jaunes Groupe* » collecte les adresses IP associées aux contenus, date et heure des requêtes effectuées sur son portail[626]. Il affirme que quand bien même la société soutient que cette collecte est justifiée par la nécessité de répondre aux demandes d'informations des autorités judicaires et administratives, celle-ci « *porte atteinte aux droits fondamentaux des personnes* »[627]. En effet, alors que le site web enregistre toutes les adresses qui se connectent à lui, le Conseil d'État souligne bien que ce traitement ne répond à aucune obligation légale et méconnait donc bien la loi Informatique et libertés alors que les données collectées sont inadéquates, non pertinentes et excessives au regard de la finalité poursuivie par le site.

Ainsi est jugée illégale la mise en mémoire de toute adresse qui souhaite se connecter à un site web. Il est argué de la généralité du procédé qui ne peut être justifié par aucune finalité d'ordre public[628]. Cette position doit toutefois être critiquée.

317. **La mémorisation nécessaire des connexions**. En effet il faut s'extraire du champ d'application de la protection des données personnelles et opérer une distanciation nécessaire entre le monde physique et l'espace dématérialisé qu'est le réseau. Dans le monde physique il est un rapport entre l'individu et le commerçant en dehors de toute mise en œuvre d'un système de vidéosurveillance : le commerçant interagit avec l'individu et est à même de rendre compte des caractéristiques de celui-ci, que ce soit les traits de son visage ou ses manières de faire. Il peut garder en mémoire ces éléments. Sur le réseau, cette interaction

[626] Conseil d'État, 10ème et 9ème sous-sections réunies, décision du 12 mars 2014, n°353193.

[627] *Ibid.*, point n°15.

[628] Le même raisonnement est tenu par la suite dans l'arrêt de la CJUE dit « *Breyer* » (CJUE (aff. C-583/14), 19 octobre 2016, *Patrick Breyer c/ Bundesrepublik Deutschland*) et celui de la Cour de cassation dit « *Logisneuf* » (Cass., civ. 1ère.,3 nov. 2016, 15-22595, *Cabinet Peterson c/ groupe Logisneuf et autres*). V. : PERONNE G., DAOUD E., « L'adresse IP est bien une donnée à caractère personnel », *D. IP/IT*, 120, février 2017.

physique n'existe pas mais elle est établie par la visualisation de l'adresse IP qui engage l'internaute.

Ainsi le principe doit être qu'elle peut être gardée en mémoire librement, de la même manière qu'un commerçant peut se souvenir d'un individu à qui il a eu affaire. Certes il y a une mise en mémoire informatique, mais l'automatisme du procédé n'a pas à être condamné en soi. Les prescriptions de la circulaire du 22 octobre 1996 suivant de peu la définition du régime de vidéosurveillance par la loi du 21 janvier 1995 peuvent apporter un éclairage intéressant. En effet, il est précisé que l'autorisation est nécessaire dès lors que les images sont transmises à un poste central quand bien même elles ne sont pas enregistrées ; en revanche il est rappelé que sont bien exclus du régime d'autorisation les simples écrans de visualisation installés à la vue de tous[629]. Or en l'espèce ici il apparaît que la mémorisation d'adresses IP renvoie à cette nécessaire visualisation qui ne peut intervenir qu'en conservant ces données techniques et évanescentes.

Cette mémorisation des connexions via des fichiers journaux ou « log-files » d'adresses IP est le propre du réseau et n'est pas liberticide ; au contraire la collecte de ces données permet d'assurer le fonctionnement des sites du web et la traçabilité nécessaire des connexions.

2) Une conservation limitée des données visant le fonctionnement du service

318. **La sauvegarde de l'intégrité du fonctionnement d'un réseau local ou d'un site web.** L'administrateur d'un réseau local ou d'un site web doit pouvoir enregistrer les adresses qui se connectent au système mis en œuvre. Il faut d'emblée considérer que cette collecte ne vise pas la surveillance individualisée d'un internaute alors que ces adresses ne sont pas pérennes dans le temps. Un site web, pour considérer une éventuelle reconnexion et des schémas de navigation sur son service, doit implanter un cookie dans l'ordinateur de l'internaute. L'administrateur d'un réseau local comme l'intranet d'une entreprise ou l'ENT d'une université, peut pour sa part considérer les données associées aux droits d'accès mis en œuvre. Ces deux procédés renvoient au régime du suivi de la navigation de l'internaute[630].

Ainsi la mémorisation systématique des adresses IP se connectant à un site web ou à un réseau local vise la pérennité du fonctionnement du site ou du sous-réseau : il

[629] Circulaire du 22 octobre 1996 relative à l'application de l'article 10 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (décret sur la vidéosurveillance), JORF du 7 décembre 1996, p. 17835. V. notamment les points 2.1 et 2.2 sur le champ d'application de la loi.

[630] V. *infra* : Titre II, Chapitre 2 : « Les conditions du suivi de la navigation de l'internaute ».

faut pouvoir détecter toute connexion anormale à celui-ci qui peut laisser présager d'une attaque informatique ou du maintien frauduleux dans le système automatisé de données. L'idée est ici de parer à toute attaque ou de considérer le blocage d'une adresse suspecte. L'identification de l'internaute qui se connecte n'intervient que dans un second temps si sont mises en œuvre des poursuites pénales pour sanctionner les infractions relatives aux « *atteintes aux systèmes de traitement automatisé de données* » et notamment celles prévues aux articles 323-1 à 323-3 du Code pénal.

Alors seulement l'article L34-1 du CPCE pourra jouer ; dans le cadre de l'instance pénale mise en œuvre, l'entreprise privée pourra obtenir les coordonnées de l'abonné et la localisation du point d'accès utilisé en vue de l'identification et de la sanction du pirate ou du « hacker » selon un anglicisme consacré[631].

319. **Le délai court de conservation des adresses IP collectées**. De fait il apparaît que la conservation de ces données n'a de sens techniquement que s'agissant d'un délai court pour considérer une menace éventuelle visant l'intégrité du site web ou une connexion frauduleuse à un réseau local administré qui se répète dans un délai court. La surveillance ici appelle à une immédiateté de la détection des connexions qui apparaissent suspectes ou frauduleuses. Une conservation longue n'est pas opérante puisque au-delà d'un an les adresses IP collectées ne peuvent plus être associées au point d'accès en considération du délai prescrit par le décret d'application de l'article L34-1 du CPCE.

En réalité la logique de tels traitements est celle du « fichier journal » ou « log file » qui enregistre de manière journalière les connexions et permet de considérer ces données dans un délai limité de quelques jours ou semaines, alors que par ailleurs un tel stockage et une telle exploitation de données ont un coût. Le principe est bien la liberté de collecte qui peut être journalière mais de fait les données collectées sont vouées à être effacées rapidement sauf détection d'une connexion suspecte. La problématique ici est en réalité celle de la mise en œuvre d'une telle collecte par les pouvoirs publics qui peuvent considérer la localisation du point d'accès dans le cadre d'une réquisition administrative ; une collecte qui organise donc une surveillance des internautes souhaitant accéder à un site ou service du web.

[631] Pour une affaire dont les faits ont permis la constatation d'un accès frauduleux dans un système de traitement automatisé de données réprimé à l'article 323-1 du Code pénal et soulevé la question du vol de données alors que l'article L323-3 n'était pas encore entré en vigueur, v. : TGI Créteil, 11ème ch. correctionnelle, jugement du 23 avril 2013, Min. public / Olivier L. (disponible sur le site Legalis.net) et l'arrêt de Cassation en date du 20 mai 2015, Cass. crim., 20 mai 2015, n°14-81336, *Bull. crim.* 2015, n°119. Sur cet arrêt, v. : CHAUVIN E., « Hacker n'est pas jouer, maintien et vol de données dans un système automatisé de traitement de données », *LPA*, 29 juillet 2015, n°150, p.15.

B] L'encadrement de tout procédé de surveillance mis en œuvre par les pouvoirs publics

320. L'**enjeu d'une surveillance des connexions au réseau.** L'enjeu de la collecte d'adresses IP circulant sur le réseau s'agissant des pouvoirs publics a peu de sens au regard de la mise en œuvre d'une opération de police judiciaire alors qu'il faut considérer qu'une simple connexion à un site ne peut réaliser une infraction. **(1).** En réalité l'enjeu de la collecte par les pouvoirs publics d'une adresse IP n'est pas celui du constat d'une infraction mais celui de l'identification d'un internaute suspect. Il renvoie au pouvoir préventif de la police administrative. Le procédé de surveillance de toutes les connexions à un site du web ne peut ainsi répondre que d'un régime d'habilitation **(2).**

1) Le non-sens d'une opération de police judiciaire visant la simple connexion à un site web

321. **L'accès au fichier-journal éventuellement mis en œuvre par l'administrateur du site ou du réseau local**. Alors qu'il est soutenu dans cette étude qu'un site web ou un réseau local doit être libre d'enregistrer toutes les adresses qui se connectent à ses services, on doit dès lors affirmer que dans le cadre d'une opération de police judiciaire, les administrateurs de tels fichiers doivent coopérer avec les pouvoirs publics et mettre à disposition les données.

Ici l'objectif de police judiciaire vise le constat d'infractions et la recherche des auteurs de celles-ci. Si des « fichiers-journaux » ont été mis en œuvre, les officiers de police judiciaire dans le cadre d'une enquête pénale visant par exemple la fermeture d'un site illicite vont pouvoir y accéder. Ainsi il est plusieurs exemples où la coopération judiciaire entre États a permis de démanteler des sites d'images pédopornographiques. Les autorités françaises ont alors pu considérer les adresses IP s'y étant connectées attribuées par un fournisseur d'accès français. Alors que la consultation habituelle de telles images est depuis 2007 érigée en infraction, des poursuites s'agissant des internautes à l'origine de telles consultations ont pu être mises en œuvre.

322. **L'utilité limitée pour les autorités françaises de l'accès à un tel fichier**. Or on le voit alors que seule cette infraction de consultation est réprimée par le droit français, la possibilité pour les pouvoirs publics de l'accès à de telles données est limitée. L'inconstitutionnalité évidente de la même infraction s'agissant de la consultation de sites à caractère terroriste fondée sur la liberté de communication[632] révèle en réalité le non-sens

[632] Conseil constitutionnel, Décision n°2016-611 QPC du 10 février 2017. V. *supra,* Partie 1ère, Titre II, Chapitre 2ème, Section II, §2), B] : *« L'inconstitutionnalité du délit de consultation visant les sites provoquant ou faisant l'apologie d'actes de terrorisme* ».

d'une telle pénalisation alors que l'enjeu ici est celui non pas de réprimer mais de prévenir les menaces terroristes et d'identifier leurs auteurs en amont de la réalisation de toute action.

De fait le délit de consultation ne peut se généraliser alors qu'il pose le problème à l'envers : il ne peut s'agir de sanctionner la consultation habituelle d'un site web illicite mais bien de le fermer. En revanche, si le procédé est soumis à un régime strict il peut être considéré que les pouvoirs publics puissent appréhender un individu suspect en ce sens qu'il se connecte à un site mis sous surveillance par les pouvoirs publics.

2) La mise en œuvre d'une opération de police administrative visant la surveillance de toutes les connexions à un site web

323. **La mise en œuvre d'un système automatisé de collecte au titre de l'article 851-3 du Code de la Sécurité intérieure.** Cette possibilité est prévue à l'article L851-3 du Code de la Sécurité Intérieure depuis la loi de 2015 relative au renseignement[633]. Cet article énonce que « *Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, il peut être imposés aux opérateurs et aux personnes mentionnés à l'article L851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste* ».

S'agissant de cet article, l'exposé des motifs de la loi explique ainsi que « *pour les seuls besoins de la lutte contre le terrorisme […], le Premier ministre peut ordonner aux opérateurs de communications électroniques et aux fournisseurs de services de détecter, par un traitement automatique, une succession suspecte de données de connexion, dont l'anonymat ne sera levé qu'en cas de menace terroriste* »[634]. Il s'agit donc bien de venir imposer aux acteurs du réseau la collecte des données qui opèrent des connexions à leurs services pour prévenir une menace terroriste, ce qui peut impliquer l'identification de l'internaute connecté.

Autrement dit un site ou une boucle du réseau peut être placée sous surveillance, les services de l'État enregistrent les adresses IP qui s'y connectent et peuvent le cas

[633] la LOI n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF du 26 juillet 2015, texte 2 sur 49.
[634] Assemblée Nationale, n°2669, projet de loi relatif au renseignement.

échéant faire le lien avec le point physique de connexion utilisé par le truchement de l'accès administratif aux données de connexions prévu à l'article L851-1.

324. **Le régime de la mise en œuvre d'un tel traitement de données**. Or la technique fait peur : le caractère sensible des « *métadonnées* »[635] collectées par ces « *boîtes noires algorithmique* »[636] est mis en avant alors que la technicité de celles-ci rend les risques eu égard aux informations dévoilées difficiles à appréhender[637]. Dans le cadre de la saisine du Conseil constitutionnel, les députés requérants s'inquiètent ainsi de l'insuffisance des garanties concernant les « *faux-positifs* »[638]. Toutefois cette technique de renseignement est déclarée conforme à la Constitution : le régime d'autorisation et la procédure de mise en œuvre prescrite font qu'elle ne porte pas une atteinte manifestement disproportionnée au respect de la vie privée[639].

En effet, la procédure pour mettre en œuvre un tel relevé des adresses IP circulant sur le réseau obéit donc au régime désormais général et codifié de toute opération de renseignement. Pour qu'une conciliation s'opère avec le « *respect de la vie privée, dans toutes ses composantes notamment le secret des correspondances, la protection des données personnelles, et l'inviolabilité du domicile* »[640], ces opérations de renseignement doivent être nécessaires aux intérêts fondamentaux de la Nation énoncés par la loi[641] ; elles doivent être soumises à un régime d'autorisation, mises en œuvre par des agents individuellement désignés et habilités et selon une procédure spécifiée et enfin être proportionnées au but poursuivi[642]. Par ailleurs une autorité administrative indépendante est instituée pour les contrôler, la CNCTR pour « *Commission Nationale de Contrôle des Techniques de Renseignement* »[643]. Le Conseil d'Etat est l'organe juridictionnel compétent s'agissant des recours visant les décisions prises[644].

---

[635] MASTOR W., « La loi sur le renseignement du 24 juillet 2015 : « La France, Etat de surveillance ? », *AJDA* 2015, p. 2018.

[636] *Ibid.*

[637] La professeure Wanda MASTOR rappelle ainsi que « Pour les détracteurs de la loi, la collecte de ces dernières serait encore plus attentatoires aux libertés que les données elles-mêmes. En résumé, ce n'est plus seulement le contenu d'un e-mail qui est collecté mais toutes les informations qui lui sont relatives : l'adresse, l'heure et le support de l'envoi etc. La collecte des métadonnées n'est en réalité ni moins, ni plus intrusive que celle des données en elle-mêmes, tant il est difficile de dissocier les deux».Wanda MASTOR, *op. cit.*

[638] Conseil constitutionnel, Décision n°2015-713 DC, du 23 juillet 2015 (Loi relative au renseignement), cons. n°59. Un faux-positif est un résultat à un test déclaré positif à tort, là où il est en réalité négatif. Il faut effectivement souligner ici la vitesse de l'adressage dynamique du réseau qui peut amener à de tels résultats. V. : F.MACREZ et J.GOSSA, « Surveillance et sécurisation ce que l'Hadopi rate, à propos de la « petite loi » « création et internet », *RLDI,* juin 2009, n°50, p.79.

[639] *Ibid.*,cons. n°58 à 60.

[640] Article L801-1 du CSI.

[641] V.TITRE Ier : « Dispositions générales », notamment l'article L811-3 du CSI

[642] V. TITRE II : « De la procédure applicable aux techniques de recueil de renseignement soumises à autorisation ».

[643] V. TITRE III. « De la commission nationale de contrôle des techniques de renseignement ».

[644] V. TITRE IV : « Des recours relatifs à la mise en œuvre de techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État ».

325. **La procédure permettant la mise en œuvre d'une telle technique**. Le relevé d'adresses IP circulant sur le réseau doit donc être autorisé par le Premier ministre après avis de la CNTCR sur le traitement mis en œuvre et les paramètres de détection retenus[645]. L'autorisation n'est valable que deux mois[646]. Elle peut être renouvelée pour quatre mois mais la demande de renouvellement doit comporter un relevé du nombre d'identifiants signalés et une analyse de la pertinence de ces signalements.

Si les données semblent caractériser l'existence d'une menace terroriste, la concordance avec un individu via l'accès au fichier des points d'accès détenus par les opérateurs en application de l'article 851-1 doit être autorisée par le Premier ministre ou l'une des personnes à qui il a délégué cette autorité[647]. Ces données ne peuvent être exploitées que pendant 60 jours après leur recueil et sont détruites à l'expiration de ce délai, sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste attachée à une ou plusieurs personnes concernées[648]. Ce recueil d'informations ne peut jamais faire l'objet d'une procédure d'urgence qui permet de mettre en œuvre le traitement avant l'avis de la CNCTR[649].

§2) L'obligation de conserver toute adresse IP à l'origine de la création d'un contenu

326. **Le régime de l'article 6 de la LCEN.** Le 1er Août 2000, alors que le web participatif se développe et que tout à chacun peut désormais mettre en ligne du contenu, la France se dote d'une législation claire sur la responsabilité des intermédiaires techniques de l'internet[650]. Ce régime de responsabilité initialement inséré à l'article 43-8 de la loi de 1986 sur la liberté de communication, est refondu en 2004 dans l'article 6 de la loi pour la Confiance en l'économie numérique. Il est ainsi décidé dans un I. d'un régime de responsabilité dit « *a posteriori* » des hébergeurs de contenus ; ils ne peuvent en effet logiquement être tenus responsables, ni civilement, ni pénalement, des contenus, alors que la mise en ligne de ceux-ci n'est pas de leur fait[651]. Cependant dès lors qu'ils sont notifiés du

[645] V. Article L851-3, II, alinéa 1 du CSI.
[646] V. Article L851-3, II, alinéa 2 du CSI.
[647] Article L851-3, IV.
[648] *Ibid.*
[649] Article L851-3, V.
[650] V. : Loi n°2000-719 du 1er Août 2000 modifiant la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication, J.O. n°177 du 2 Août 2000, p. 11903. Cette loi transpose la directive dite « commerce électronique » du 8 juin 2000 (Dir. 2000/31/CE).
[651] V. : l'article 6.I.2 visant leur responsabilité civile et l'article 6.I.3 visant leur responsabilité pénale.

caractère illicite du contenu mis en ligne[652], ils sont tenus de le supprimer[653]. Ils ne sont pas non plus soumis à une obligation générale de surveiller les informations stockées ni de rechercher les faits ou les circonstances révélant des activités illicites[654].

En revanche, en application du II., ils sont tenus de conserver « *les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* » afin que la responsabilité de l'auteur de la mise en ligne puisse, elle, être mise en œuvre.

327. ***Plan***. Il sera vu que ce régime qui vise d'une manière générale des « *données de nature à permettre l'identification* » doit être clarifié **(A).** Les services du web peuvent librement collecter des renseignements sur l'internaute ; en revanche, ils doivent être contraints de conserver toutes les adresses IP à l'origine de contenus, données techniques qui réalisent le lien nécessaire avec le monde physique et le point de connexion utilisé **(B).**

A] La nécessaire clarification du régime de l'identification de tout créateur de contenus prévu par la LCEN

328. **Les données visées par l'article 6.II de la LCEN**. Les données à conserver « *de nature à permettre l'identification* » de tout créateur de contenus ne sont pas détaillées par la loi qui prévoit un décret d'application à cet endroit. Celui-ci sera pris en 2011 seulement[655]. Il vise en premier lieu la conservation de « *l'identifiant de la connexion* » mais également la conservation de données qui ne sont pas techniques, à savoir « *les informations fournies lors de la souscription, d'un contrat par un utilisateur ou lors de la création d'un compte* ». Par ailleurs l'alinéa 2 du II de l'article 6 oblige les hébergeurs à fournir à leurs clients ou utilisateurs *« des moyens techniques leur permettant de satisfaire aux conditions d'identification prévues au III de ce même article* ».

En effet l'article 6.III considère la nécessité de tenir à disposition du public des informations identifiant l'éditeur de contenus dans la droite ligne des prescriptions du droit de la presse. Pour les éditeurs non professionnels, afin de « *préserver leur anonymat* »[656] il est prévu que « *les éléments d'identification personnelle* » ne soient

[652] Pour le détail des éléments requis afin de notifier un contenu illicite : v. art. 6.I.5 de la LCEN. Il est à noter que le paragraphe 6.I.4 sanctionne pénalement « *le fait pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte* ».

[653] Article 6.I.2 de la LCEN.

[654] Article 6.I.7 de la LCEN.

[655] V. Décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

[656] V. article 6.III. 2. de la LCEN.

transmis qu'à l'hébergeur ; la seule mention de ce prestataire apparaissant alors sur la page web.

329. ***Plan.*** Ainsi l'article 6.III de la LCEN oblige originellement à ce qu'un minima de données soit collecté auprès de l'internaute pour qu'il puisse éditer du contenu en ligne, une obligation qui aujourd'hui, à l'heure du web applicatif et de la multiplication des comptes-utilisateurs, apparaît désuète **(1).** Or cette logique d'une collecte d'informations est aujourd'hui rendue obligatoire par le décret d'application de l'article 6.II de la LCEN. Il faut dénoncer l'inefficacité de celui-ci alors qu'il devrait s'en tenir à la conservation de données techniques garantissant qu'un contrôle de l'identité de l'internaute connecté puisse être mis en œuvre **(2).**

1) La désuétude de l'article 6.III de la LCEN

330. **L'obligation de collecte d'informations personnelles prévue par l'article 6.III de la LCEN**. En France l'apparition du web 2.0 a suscité des interrogations. La loi du 1er Août 2000 modifiant la loi de 1986 sur la liberté de communication a ainsi encadré l'identification des éditeurs de contenus, en distinguant les professionnels des non-professionnels, pour lesquels a été ménagée une possibilité d'anonymat. En effet ces derniers sont soumis à une obligation médiate[657] : ils peuvent ne pas faire apparaître leurs coordonnées sur la page web sur laquelle ils s'expriment à condition qu'ils tiennent celles-ci à la disposition de l'hébergeur[658]. Alors qu'il était à l'esprit de tous que l'internaute pouvait communiquer des coordonnées fantaisistes[659], la tentation a pu être de requérir l'identité civile de l'internaute. Un amendement[660], heureusement non adopté, avait été déposé qui visait à pénaliser toute fausse déclaration d'identité.

En effet l'objectif n'est pas de contrôler le propos de l'internaute en l'obligeant à dévoiler son identité et ce quand bien même au seul hébergeur ; une politique de ce type dite de « *real names* » ou « *nom réel* », qui peut avoir cours dans certains pays comme la Chine et la Corée du Sud, est nécessairement attentatoire à la liberté d'expression de l'internaute et donc inconstitutionnelle **(a).** En France, l'article 6.III de la LCEN oblige

[657] CACHARD O., L'obligation d'identification dans la loi du 1er Août 2000 (modifiant la loi du 30 septembre 1986 relative à la liberté de communication », article mis en ligne le 1er octobre 2000 sur le site du CEJEM, cejem.com

[658] V. le nouvel article 43-10 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication, tel que créé par l'article 1er de la loi n°2000-719 du 1er Août 2000, qui complète la loi de 1986 par un nouveau chapitre VI intitulé « *Dispositions relatives aux services de communication en ligne autres que de correspondances privée* ».

[659] Ainsi de la célèbre affaire Tiscali, le contributeur avait renseigné ses coordonnées comme telles : -Nom : Bande - Prénom : Dessinée, -Adresse : rue de la BD659. CASS. 1ère civ., 20 janvier 2014 , *Tiscali Média c/ Dargaud Lombard, Lucky Comics*

[660] « Amendement Bloche à la loi sur l'audiovisuel : les internautes devront s'identifier avant d'émettre du contenu. », article mis en ligne le 27.03.2000, sur le site *legalnews.fr*, rubrique « Communication & NTIC ».

simplement à la mise en œuvre de formulaires de comptes détaillés ; une obligation à visée pédagogique peu respectée toutefois car s'inscrivant à rebours du développement du web 2.0 **(b).**

a. L'inconstitutionnalité des politiques dites de « real names » ou « nom réel ».

331. **Le principe d'une politique dite de « *real names* » ou de « *nom réel* ».** Il est certains États comme la Corée du Sud et la Chine[661] qui ne s'en tiennent pas à l'identification permise par la localisation du point d'accès et l'investigation que celle-ci permet. Ils exigent de leurs ressortissants qui souhaitent mettre en ligne du contenu sur le web qu'ils s'identifient à priori de toute mise en ligne, auprès du fournisseur de services[662], via pour ce faire leur numéro d'identification national[663]. C'est ce qu'on appelle une politique de « *real names* » ou « *nom réel* »[664] en français.

En ce sens il faut différencier ces politiques publiques de celle du réseau social Facebook parfois dite elle aussi de « *real names* » alors qu'elle interdit l'usage de pseudonymes sur son réseau[665]. Nous ne souscrivons pas à cette assimilation alors que techniquement un internaute peut renseigner un pseudonyme sur le réseau social sans que cela bloque son profil ; ce qui est prohibé et traqué par la firme californienne est en réalité la création de faux profils qui vont à l'encontre de l'objectif du site de mettre en relation des individus.

Ce qu'il faut encadrer est le pouvoir des autorités publiques de faire coïncider les procédés d'authentification du web avec le système d'identification des individus qu'ils mettent en œuvre à l'échelle nationale qui est pérenne et effectif.

332. **L'atteinte disproportionnée à la liberté d'expression de l'internaute**. Un individu ne peut être forcé de décliner son identité avant toute prise de parole ; l'expression « prise de

[661] David A. CARAGLIANO, « Real names and responsible speech : the cases of South Korea, Russia, and Facebook », working draft, *The Right to Information & Transparency in the Digital Age*, Stanford University, March 11-12, 2013; D.LELOUP et L.CHECOLA, « L'anonymat proscrit des réseaux sociaux à Pékin », article mis en ligne le 16.03.2012 sur le site *LeMonde.fr*.

[662] Notamment s'agissant des sites de micro-blogging comme le site *Sina Weibo* en Chine, l'équivalent chinois de *Twitter*. En Corée du Sud, les sites concernés sont notamment *Yahoo ! Korea, Daum communications, NHN and NeoWiz.* Il est à noter que Google a refusé en Corée du Sud de se soumettre à cette politique et a décidé de désactiver toute forme de contribution sur YouTube pour les internautes sud-coréens. V. « YouTube ne veut pas demander la carte d'identité de ses utilisateurs », article publié le 14.04.2009 sur le site numerama.com

[663] En Corée du Sud la loi requiert des internautes qu'ils indiquent leur « *Resident Registration Number* », autrement dit leur numéro de résident qui est un numéro identifiant à l'échelle nationale. V. V. David A. CARAGLIANO, « Real names and responsible speech : the cases of South Korea, Russia, and Facebook »,*op.cit*,

[664] Cette expression est utilisée dans l' « Etude mondiale sur le respect de la vie privée sur Internet et la liberté d'expression ». Etude réalisée par T.MENDEL et al, et publiée en 2013 aux éditions Unesco (Paris, coll. Unesco sur la liberté de l'Internet), p.67

[665] V. David A. CARAGLIANO, « Real names and responsible speech : the cases of South Korea, Russia, and Facebook », working draft, *The Right to Information & Transparency in the Digital Age*, Stanford University, March 11-12, 2013

parole » est utilisée ici à dessein alors que la logique, quand bien même ces paroles se réalisent dans un support écrit ou vidéo, n'est pas celle de l'édition d'un contenu à titre professionnel. La distinction doit s'opérer alors que le réseau doit être considéré comme un nouvel espace et non comme un nouveau support de publication. Ainsi les juges de la Cour constitutionnelle sud-coréenne ont estimé à l'unanimité que la loi mise en œuvre était inconstitutionnelle en rappelant que l'objectif de celle-ci visant à décourager les discours illicites et à en retrouver les auteurs était pleinement atteint par la collecte de l'adresse IP à l'origine du contenu et la mise en œuvre d'une investigation légale[666].

Selon la même logique, aux États-Unis, la Cour d'appel du 9ème circuit a confirmé en 2014 l'injonction qui avait suspendu l'application d'une disposition de loi adoptée par référendum par les électeurs de l'État de Californie, le 6 novembre 2012[667]. Celle-ci visait à obliger toute personne condamnée pour un délit sexuel à faire connaître à la police tous les identifiants utilisés sur des sites en ligne pour communiquer avec des tiers, ainsi que les coordonnées du FAI utilisé, et ce sous peine d'emprisonnement. Les juges fédéraux ont affirmé qu'une telle prescription constituait une violation du 1er amendement de la Constitution américaine garantissant la liberté d'expression (« *Right to free and anonymous speech* ») et précisé que leur décision d'interdire cette identification auprès des services de police n'entravait en rien la capacité de l'État à enquêter sur les délits à caractère sexuel qui pouvaient être commis en ligne. L'état de Californie a décidé de ne pas porter l'affaire devant la Cour suprême.

Alors que la France n'a jamais requis de l'internaute souhaitant s'exprimer en ligne qu'il atteste de son identité, l'article 6.III de la LCEN a toujours eu une visée pédagogique qui a de fait peu de sens.

b. La problématique des formulaires de comptes succincts du web 2.0

333. **Les prescriptions de l'article 6.III.2 de la LCEN**. La LCEN en 2004 reprend les prescriptions adoptées en 2000 et oblige dans son article 6.III.2 les éditeurs non

[666] La décision de la Cour constitutionnelle sud-coréenne date du 23 Août 2012. V. : David A. CARAGLIANO, « Real names and responsible speech : the cases of South Korea, Russia, and Facebook »,*op.cit ;* l' « Etude mondiale sur le respect de la vie privée sur Internet et la liberté d'expression », réalisée par T.MENDEL et al, *op.cit,* p.67 ; « La Corée revient sur un dispositif requérant l'identification des internautes », article mis en ligne le 27.08.2012 sur le site *LeMonde.fr. ;* « Sorting out the Net », article mis en ligne le 24 Août 2012 sur le site du quotidien *koreajoongangdaily.joins.com.*

[667] V. : Après une première décision du juge ayant suspendu temporairement la « proposition 35 » au lendemain du référendum, la Cour de district confirme sur le fond cette décision (V. : United States District Court, for the Northern District of California, N°C12-5713 TEH, *Order granting plaintiff's motion for a preliminary injuction in Doe v. Harris)*. L'État Californien fait appel de cette décision ; la Cour d'appel du 9ème circuit se prononce le 18 novembre 2014 (V. : Doe v. Harris, No. 13-15263 (9th Cir. 2014)). V. pour des liens actifs vers ces décisions les communiqués de presse de l'EFF (Electronic Frontier Fondation, organisation sans but lucratif de protection des libertés sur Internet, basée à San-Francisco), disponibles sur leur site : eff.org.

V. également : BERNE X. « En Californie, les délinquants sexuels obligés de se dévoiler sur le Net », article mis en ligne le 6 novembre 2012 sur le site *nextinpact.com* ; CHAMPEAU G. « La Loi contre l'anonymat suspendue par la justice californienne », article mis en ligne le 7 novembre 2012 sur le site *numerama.com.*

professionnels à communiquer à l'hébergeur leurs « *nom, prénoms, domicile et numéro de téléphone* »[668] ; leur page dès lors n'a à mentionner que « *le nom, la dénomination ou la raison sociale et l'adresse* » du prestataire d'hébergement et ce pour « *préserver leur anonymat* ». Cet article impose donc aux services de communication en ligne de requérir ces informations au moment de la création d'un compte utilisateur.

Or dans les premières années du web 2.0 ces informations ne sont pas toujours requises ; les sites s'en tenant parfois au choix d'un simple « *login* » ou nom d'utilisateur et mot de passe. Cette politique visant à la démocratisation des services du web 2.0 a été condamnée en ce qu'elle ne respectait pas les prescriptions de la loi française[669].

334. **La problématique des formulaires création de compte succinct du web dit « participatif ».** La problématique était alors la suivante : des ayants-droits constatant la mise en ligne de contenus contrefaisants, notamment sur les plateformes-vidéos, en plein essor à l'époque, telles « *YouTube* » et « *Dailymotion* », saisissaient le juge afin qu'il requiert de l'hébergeur, sur le fondement de l'article 6.II, « *les données de nature à permettre l'identification de quiconque a contribué à la création du contenu*». Ces derniers ne communiquaient alors qu'une simple adresse IP considérant remplie l'obligation alors que le décret devant préciser les données à conserver pour ce faire n'était pas encore pris. Dès lors charge aux ayants-droits et charge financière surtout, de saisir le juge pour que sur le même fondement de cet article 6.II, le FAI divulgue les coordonnées de l'abonné à l'origine de la mise en ligne.

Il a été soutenu par l'auteur de cette étude qu'il fallait faire prendre conscience à l'internaute de l'enjeu de sa prise de parole en ligne en détaillant les formulaires de création de compte. En attente du décret de l'article 6.II, les prescriptions de l'article 6.III devaient être respectées par les sites web qui, *a minima,* en plus de la conservation de l'adresse IP, devaient organiser l'architecture de leur formulaire de compte de manière à ce que les mentions du « *nom, prénoms, domicile et numéro de téléphone* » apparaissent. Il ne devait pas être permis au créateur de contenus de « *n'avoir même pas à fournir des données fantaisistes* »[670].

[668] Article 6.III de la loi n°2004-575 du 21 juin 2004 pour la confiance en l'économie numérique.

[669] V. la position de l'auteur de cette étude *in* CRIQUI G., « La fourniture d'une simple adresse IP est-elle suffisante ? Ou quand l'obligation à la charge de l'hébergeur doit être précisée. », *RLDI*, 05/2009, perspectives-analyse n°49.

[670] CRIQUI G., « La fourniture d'une simple adresse IP est-elle suffisante ? Ou quand l'obligation à la charge de l'hébergeur doit être précisée. », *op. cit.*

335. **La désuétude de cette l'obligation de détail du formulaire de création de compte**. Aujourd'hui il faut toutefois constater que cette position appliquant à la lettre les dispositions de la loi s'inscrivait à rebours de la démocratisation de tels services permise par cette facilité de mise en ligne qui les caractérisent et qui ne peut être condamnée *per se*. De fait actuellement, la logique est inverse, le web applicatif met en relation des profils détaillés via la création de comptes-utilisateurs ; procédé qui en soi non plus ne peut être condamné. Alors que la logique d'identification de l'internaute à partir de son adresse IP est aujourd'hui mieux comprise, la visée pédagogique de l'article 6.III apparaît aujourd'hui comme désuète.

2) La confusion opérée par l'article 6.II de la LCEN

336. ***Plan.*** Selon la même logique l'article 6.II de la LCEN qui organise de manière générale la conservation de « *données de nature à permettre l'identification de quiconque a contribué à la création du contenu* » fait apparaître une malfaçon alors qu'il faut dissocier le contrôle de l'identité de l'internaute connecté des procédés permettant une possible interaction avec un créateur de contenus.

Il faut souligner ainsi l'ineffectivité du décret d'application de l'article 6.II de la LCEN pris en 2011 puisqu'il ne dissocie pas la nécessaire obligation de conservation de données techniques vouées à être effacées, de l'accès à des informations personnelles qui de fait en application du droit commun, si elles sont collectées et conservées par les sites du web, doivent être tenues à disposition des autorités compétentes **(a).** A cet endroit il apparaît qu'il faille réfléchir à un nouveau régime visant le « *pseudonymat* » de l'internaute qui doit être dissocié de celui visant les conditions du contrôle de son identité **(b).**

a. L'ineffectivité du décret d'application n°2011-219

337. **L'article 1er du décret n°2011-219.** Le dernier alinéa du II de l'article 6 de la LCEN précise qu'un décret en Conseil d'État pris après avis de la CNIL définit les données mentionnées au premier alinéa de cet article 6.II et détermine la durée et les modalités de leur conservation. Longtemps attendu, il s'agit du décret n° 2011-219 du 25 février 2011 « ***relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne »***[671].

[671] Ce décret a été modifié s'agissant de la conservation des données permettant de vérifier le mot de passe ou de le modifier par le décret n°2012-436 du 30 mars 2012 portant transcription du nouveau cadre règlementaire européen des communications électroniques.

Celui-ci précise dans son article 1er 2° que les hébergeurs[672] doivent conserver « *pour chaque opération de création* » –de contenus- : « *l'identifiant de la connexion à l'origine de la communication »* et les données techniques qui lui sont associées. Et il faudrait s'en tenir là. Or le 3° les enjoint également à conserver « *les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte* » : à savoir l'identifiant à l'origine de la connexion qui a permis la création du compte mais également les informations renseignées par l'internaute pour créer ce compte utilisateur. Sont visés : « *les nom et prénom ou sa raison sociale* », « *les adresses postales associées* », « *les pseudonymes utilisés* », « *les adresses de courrier électronique ou de compte associées* », « *les numéros de téléphone* » et enfin « *le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour* ».

Il est indiqué toutefois que s'agissant de telles données : elles « *ne doivent être conservées que dans la mesure où les personnes les collectent habituellement* ». Cette précision fait apparaître le caractère ineffectif des prescriptions du 3° de cet article 1er : les données renseignées par l'internaute qui ne sont pas des données techniques, impermanentes par nature, n'ont pas à répondre d'un régime d'ordre public qui organise leur conservation en vue de ménager l'identification des internautes créateurs de contenus.

338. **La mise en œuvre de l'obligation d'identification : une simple adresse IP suffit**. De la même manière que pour les données collectées dans le cadre de la mise en œuvre de droits d'accès à un réseau local, le mécanisme du compte-utilisateur mis en œuvre par les sites du web ne permet pas d'attester de l'identité de l'internaute connecté ; il réalise simplement une authentification de celui-ci[673]. Par ailleurs la teneur des données collectées doit être libre et ne peut être corrélée de manière générale avec des documents d'identité[674].

Ainsi ces données peuvent évidemment aider à l'identification de l'internaute à l'origine de la mise en ligne mais ne la garantissent jamais. Disant cela une problématique nouvelle apparaît alors que s'agissant de ces données collectées librement par les sites du web qui peuvent révéler l'identité réelle de l'internaute s'exprimant via un pseudonyme, il convient de considérer dans quelle mesure celles-ci doivent faire

[672] A dessein ne seront pas détaillées ici les prescriptions du décret visant les données qui devraient être collectées par les FAI alors que ce détail n'a pas de sens s'agissant de la mise en ligne d'un contenu.

[673] V. *supra :* Titre I, chapitre 2ème, Section I, §2), A] « *La possible authentification de l'internaute connecté* ».

[674] V. *supra* n°330 et suiv.

l'objet d'un secret et peuvent donc être divulguées. Une acception nouvelle a cours aujourd'hui qui vise le respect du « *pseudonymat de l'internaute* ».

b. La problématique nouvelle du respect du « pseudonymat » de l'internaute

339. **Cette formulation nouvelle visant le « *pseudonymat* » de l'internaute.** Cette formulation qui émerge[675] est très imparfaite car en réalité ce qui est protégé est l'anonymat de l'internaute. Il ne s'agit pas bien sur de protéger la révélation du pseudonyme ou du profil créé par l'internaute comme ce néologisme le laisse entendre mais bien de considérer dans quelle mesure peut être révélée l'identité réelle de l'internaute.

Il est proposé dans cette étude de considérer que ce concept de « *pseudonymat* » doit se départir de la législation visant le traitement des données personnelles qui aujourd'hui utilise maladroitement ce terme de « *pseudonymisation* » pour être circonscrit à l'enjeu de l'expression en ligne[676]. Le respect du « *pseudonymat* » doit s'entendre de la protection qu'est en droit d'attendre un individu s'agissant de la corrélation entre son pseudonyme et les éléments de son identité qu'il a divulgué à une entreprise du web. L'enjeu ici n'est pas celui de la liberté individuelle mais celui de la liberté d'expression.

Il faut rappeler que s'agissant de la mise en ligne de contenus illicites, une procédure de retrait après notification est prévue qui permet une régulation des propos. Par ailleurs toute adresse IP à l'origine de la mise en ligne d'un contenu doit être conservée de manière à permettre le contrôle de l'identité. Or en parallèle de cette action

---

[675] V. : MALLET-POUJOL N., « Droit des communications électroniques (Mars 2017-Mars 2018) », *Légipresse* 01/04/2018 ; METALLINOS N., « Vers une garantie du pseudonymat sur les forums de discussion ? », *CCE*, mai 2017, n°48, p.32.

[676] Le RGPD définit dans son article 4. 5) la notion de « *pseudonymisation* » comme : « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires ». Cette « *pseudonymisation* », continue l'article, est réalisée : « pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles » et ce « afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

Autrement dit si cette définition, qui n'en est pas une, est remise en perspective : un traitement de données est « *pseudonyme* » lorsque les données qu'il traite ne révèlent pas directement l'identité de l'internaute mais que celle-ci peut être découverte si ces données sont mises en relation avec d'autres faisant l'objet d'un traitement différent. Dès lors la définition qui souligne l'enjeu du respect de l'individu à cet égard qui ne peut être identifié à son insu, prescrit que cette interconnexion doit répondre d'un régime strict opéré par des mesures techniques et organisationnelles. On le voit émerge ici un nouveau type de traitement qui ne vise plus des données « *anonymisées* » qui ne pouvaient plus conduire à l'identité de l'internaute, mais un traitement que l'on pourrait dire « médian » de données qui peuvent, associées avec d'autres, révéler l'identité de l'internaute.

Or à l'heure de la multiplication des traitements de données, qui numérisés facilitent l'interconnexion, cette conceptualisation est peu claire. L'enjeu de l'identification de l'internaute et celui de la surveillance de ses agissements sur le Web est dilué dans celui de la protection des données collectées. Il est ainsi énoncé que « *la pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligation en matière de protection de données* ». (Cons. 28.,du RGPD). »[676]. Or comme le soulignent A. Debet, J. Massot et N. Metallinos dans leurs ouvrage « *Informatique et Libertés* » : « *La même critique que pour le test de l'anonymat sur les limites de la définition peut être ici formulée : en effet, la nécessité du réexamen constant de la persistance du pseudonyme est difficilement compatible avec les besoins de sécurité juridique des responsables de traitement et risque de réduire considérablement les bénéfices attachés au traitement de données pseudonymes* » (DEBET A., MASSOT J., METALLINOS N., Informatique et Libertés, la protection des données personnelles en droit français et européen, L.G.D.J.,Paris, 2015, n°539, p. 265.)

qui vise l'internaute connecté au réseau et le respect de sa liberté individuelle, le respect du « *pseudonymat* » de l'internaute invite à considérer une autre problématique qui vise la liberté d'expression de l'internaute et les données qu'il a lui-même divulguées.

340. **L'enjeu d'un nouveau régime**. Actuellement la problématique est de considérer dans quelle mesure le « *pseudonymat* » de l'internaute doit être respecté alors qu'il faut s'interroger sur la possibilité que sur simple requête auprès du juge un particulier puisse considérer l'identité réelle d'un individu s'exprimant en ligne sous couvert d'un pseudonyme.

C'est l'écueil de ce régime très imparfait de l'article 6.II de la LCEN et de son décret d'application. En visant les informations personnelles, il organise le possible accès de celles-ci dans le cadre d'une requête judiciaire, selon l'alinéa 3 de du II de cet article 6 ; un terme qui renvoie donc à une procédure non contentieuse. Or cet accès, même mis en œuvre par un juge doit être questionné. A cet endroit il faut réfléchir à un nouveau régime qui doit également repenser la notion d'interaction avec l'internaute, qui doit pouvoir être joint et répondre de ses mises en ligne mais peut rester anonyme quand bien même attrait devant les tribunaux. Un nouveau mouvement apparaît, notamment aux États-Unis, qui considère comme une identité nouvelle le pseudonyme choisi, et qui protège l'intégrité de celui-ci. L'internaute doit pouvoir être condamné civilement tout en pouvant prétendre à conserver l'usage de son pseudonyme non dévoyé qui l'identifie de manière pérenne sur le web[677].

En revanche il faut bien organiser à minima la conservation de toute adresse IP à l'origine d'une mise en ligne, seule donnée tangible car procédant de l'adressage même du réseau, qui en faisant le lien avec l'espace physique du monde réel permet le contrôle de l'identité de l'internaute connecté et la mise en œuvre de poursuites pénales.

B] Le régime visant l'obligation de conserver toute adresse IP à l'origine d'une mise en ligne

[677] Aux États-Unis, depuis le début des années 2000, il est affirmé de la même manière qu'en Europe, de manière claire, que l'obtention auprès d'un FAI des coordonnées de l'auteur de propos anonymes sur un forum de discussion sur Internet ne s'apparente pas à une atteinte au 1er amendement de la Constitution américaine garantissant la liberté d'expression (Cour Suprême de l'État de Virginie, 1er novembre 2002, *AOL c./Nam tai Electronics*). Tout individu agissant sur le Web doit pouvoir être retrouvé et l'anonymat n'est jamais total sur celui-ci.

Toutefois il est aujourd'hui considéré par certains juges américains que quand bien même l'internaute a été condamné dans le cadre d'un procès civil, si les contenus litigieux ont été supprimés, l'anonymat de l'auteur des propos doit lui être garanti sur le fondement de ce premier amendement (V. la décision de la Cour d'appel américaine du 6ème circuit, *Signature Management Team, LLC v. Doe,* No. 16-2188 (6th Cir. 2017)). En l'espèce l'anonymat d'un bloggeur ne peut être levé dans le cadre de poursuites civiles alors que si le contenu litigieux a été retiré, il peut prétendre à ce que son pseudonyme ne soit pas associé à son identité réelle pour pouvoir continuer à tenir le blog qu'il a crée sous cette identité numérique qui es reconnue sur cet espace.

341. ***Plan.*** A l'heure du web applicatif, non seulement l'adresse IP à l'origine de tout contenu doit être conservée mais également celle qui opère une connexion au compte-utilisateur. La conservation de ces données n'a de sens qu'en regard du délai prescrit pour permettre la localisation du point d'accès associé **(1).** Selon la même logique ces données doivent être tenues d'une manière générale à disposition des autorités compétentes, judiciaires et administratives, pour leur permettre de considérer dans un second temps selon une procédure stricte la localisation du point d'accès utilisé **(2).**

1) Les différentes adresses IP soumises à l'obligation de conservation

342. **Le contenu du décret n°2011-219 du 25 février 2011**. Le décret précisant l'obligation de l'article 6.II de la LCEN « ***relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne »***[678] une fois son champ d'application clarifié peut servir de point de réflexion s'agissant des adresses IP à conserver. Il différencie ainsi l'obligation de conserver pour l'hébergeur « *L'identifiant de la connexion à l'origine de la communication* » de l'obligation de conserver « *au moment de la création du compte, l'identifiant de cette connexion* ». La conservation de ces adresses IP obéit alors à deux logiques différentes selon le décret. L'identifiant à l'origine de la communication doit être conservé 1an à partir de la création du contenu. L'identifiant à l'origine de la création du compte utilisateur doit être conservé 1 mois après la fermeture du compte.

Or il nous semble que ces délais ont peu de sens. D'une part on voit mal pourquoi tant que le contenu est en ligne l'identifiant de la connexion qui l'a créé n'est pas conservé ou inversement pourquoi il devrait être conservé si le contenu n'est plus en ligne. S'agissant du compte-utilisateur, s'il est rendu inactif, pourquoi conserver l'adresse IP à l'origine de sa création. De fait les comptes-utilisateurs ont aujourd'hui plusieurs années et la conservation de l'adresse IP qui a créé un compte Facebook il y a 11 ans n'a aucune pertinence alors qu'il faut bien considérer que ces adresses IP ne peuvent mener à l'identification de l'internaute à l'origine de la connexion que dans le cadre d'un rapprochement avec les données détenues par le FAI ou l'administrateur du réseau local utilisé en application de l'article L34-1 du CPCE qui répondent de la mise en œuvre d'une obligation générale de localisation des points d'accès.

[678] Ce décret a été modifié s'agissant de la conservation des données permettant de vérifier le mot de passe ou de le modifier par le décret n°2012-436 du 30 mars 2012 portant transcription du nouveau cadre règlementaire européen des communications électroniques.

343. **La nécessaire articulation du décret de 2011 précisant l'article 6.II de la LCEN et du décret de 2006 visant les données conservées au titre de l'article L34-1.** En effet, le décret n°2006-358 du 24 mars 2006 pris en application de l'article L34-1 du CPCE[679] prescrit un délai de conservation de 1an à compter du jour de l'enregistrement de l'adresse IP attribuée au point d'accès au moment de la connexion.

Ce délai de conservation qui n'est pas indéfini est justifié d'une part par la réalité physique du stockage de telles données et le coût de celui-ci alors que par ailleurs les connexions comme les contenus sur le réseau sont volatiles et qu'il est inutile de procéder à une indexation indéfinie de toutes les données de connexion au réseau.

Ainsi il apparaît que la conservation d'une adresse IP à l'origine de la mise en ligne d'un contenu est pertinente tant que le contenu est en ligne et dans la limite sinon de une année ; ce qui permet de remonter au point d'accès qui a été utilisé pour la connexion. Ce délai qui peut parfois paraitre court[680] permet en réalité de mettre en avant l'intérêt de la régulation dans le cadre d'un contentieux visant la liberté d'expression.

S'agissant du compte-utilisateur, il faut conserver non pas l'adresse IP à l'origine de sa création mais toute adresse qui se connecte au profil créé. De fait le délai de conservation tend alors à être indéfini puisque les connexions au compte-utilisateur se répètent quotidiennement. Toutefois cette conservation de toute adresse IP à l'origine d'une connexion à un profil n'est pas condamnable en ce que le contrôle de l'identité de l'internaute à partir d'une adresse IP fait l'objet d'une procédure définie qui ne peut ressortir que des pouvoirs publics.

2) La mise à disposition de telles données aux autorités compétentes.

344. **L'article 6.II alinéa 3 de la LCEN**. L'article 6.II alinéa 3 de la LCEN énonce que « L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa ». Toutefois cette prescription n'a pas de sens et peut même prêter à une confusion dangereuse.

En effet d'une part il sera vu qu'il faut fermement condamner l'application d'une telle prescription aux données détenues par les opérateurs de communications électroniques, eux aussi visés par l'article 6.II de la LCEN. Or la LCEN ne doit viser

[679] Décret n°2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques

[680] TGI Nanterre, 1ère ch., Ord. de mise en état, 1 sept. 2011, *Melle G. /Paperblog*. Dans cette affaire une actrice reproche au site *Paperblog* de reproduire une brève scène de film dans lequel elle apparaît à moitié dénudée ; elle réclame au site la production des données détenues en application de la LCEN et du décret de février 2011. Le site qui revendique le statut d'hébergeur communique les données du compte de l'auteur du contenu litigieux mais s'oppose à la mise à disposition des données de connexion alors que la demande a été formée en mai 2011 et que l'extrait de film a été publié en avril 2010.

que la collecte d'adresses IP au point d'arrivée de la communication, c'est-à-dire celles visualisées par les sites web et ne peut venir déborder les prescriptions de l'article L34-1 du CPCE qui limite la divulgation de la localisation du point d'accès à la mise en œuvre de poursuites pénales[681].

D'autre part, si l'on considère que les informations personnelles renseignées par l'internaute et leur divulgation ne peuvent ressortir de cet article pour que soit protégé le « *pseudonymat* » de l'internaute, la procédure d'une requête s'agissant de la divulgation de la seule adresse IP à l'origine de la mise en ligne ou connexion au compte-utilisateur n'a pas de sens puisque celle-ci ne révèle rien en soi. La divulgation d'une telle adresse est en réalité indissociable de la mise en œuvre d'une procédure pénale nécessaire pour accéder aux données détenues par le FAI ou l'administrateur réseau. L'hébergeur tenu de conserver une telle adresse la mettra à disposition dans le cadre de cette instance.

345. **L'article 6.II bis désormais codifié dans le Code de la Sécurité Intérieure**. Par ailleurs, en 2006, la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, a introduit dans la LCEN un article 6.II.bis qui organise l'accès de l'autorité administrative aux données collectées par les sites web au titre de l'article 6.II, à savoir les données permettant l'identification de tout créateur de contenus[682].

Depuis la loi 2013 dite de *« programmation militaire »*, cette procédure de requête administrative est prévue dans le cadre des dispositions du Code de la sécurité intérieure[683]. Au titre de l'article L851-1, dans les conditions strictes prévue au chapitre 1er du titre II du livre VIII intitulé « *Du renseignement »*[684], les services spécialisés de renseignement, qui sont désignés par décret en Conseil d'Etat, peuvent recueillir auprès des personnes mentionnées au 1 et 2 du I de l'article 6 de la LCEN « *des informations ou documents traités ou conservés par leurs réseaux ou services de communications*

[681] V. *infra* Section II. *« La procédure permettant la divulgation du point d'accès utilisé* ».

[682] LOI n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant disposition diverses relatives à la sécurité et aux contrôles aux frontières (JORF du 24 janvier 2006, p. 1129), article 6, II.

[683] LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (JORF du 19 décembre 2013, texte 1 sur 163), article 20. Il est ajouté un chapitre VI « *Accès administratif aux données de connexion* » contenant les articles L246-1 à L246-5, dans le titre IV désormais appelé « *Interceptions de sécurité et accès administratif aux données de connexion* », du livre II de la partie législative « *Ordre et sécurité publics* ». Pour la modification de la partie règlementaire, v. : Décret n°2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.

[684] Cette nouvelle numérotation date de la LOI n° 2015-912 du 24 juillet 2015 *« relative au renseignement* » (JORF du 26 juillet 2015, texte 2 sur 49) qui crée dans la partie législative du Code de la Sécurité Intérieure un livre VIII « *Du renseignement »*, qui débute par l'article L801-1 qui est suivi de neuf titres. Le Titre V s'intitule « *Des techniques de recueil de renseignement soumise à autorisation* » ; il débute par un chapitre 1er' « *Des accès administratifs aux données de connexion* », comprenant les articles 851-1 à 851-7.

électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques ».

Cet article renvoie également aux conditions de l'accès administratif aux données détenues par les opérateurs de communications électroniques. Ainsi la logique du contrôle d'identité apparaît plus clairement grâce à ce régime unifié : l'adresse IP à l'origine d'une connexion ne fait pas l'objet d'un secret mais doit être tenue à disposition des autorités administratives qui ne peuvent toutefois considérer la divulgation du point d'accès associé que selon une procédure stricte qui garantit le respect des libertés individuelles et de la vie privée de l'internaute.

Section II. La procédure permettant la divulgation du point d'accès utilisé

346. **La procédure prévue par l'article L34-1 du CPCE.** Crée en 2001, l'article L34-1 énonce à l'origine que les données détenues par les opérateurs de communications électroniques, permettant de localiser le point d'accès et donc potentiellement d'identifier l'internaute, ne peuvent être conservées et donc transmises que « *pour les besoins de la recherche, de la constatation, et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations ».*

Ainsi le point d'accès utilisé ne peut être localisé que par un officier de police judiciaire, dans le cadre d'une enquête de police judiciaire, c'est-à-dire qui vise la constatation d'une infraction et non sa prévention et qui est conduite sous la direction du procureur de la République ; une enquête qui permet le cas échéant le déclenchement de l'action publique.

Cet accès des pouvoirs publics à la localisation des points d'accès est nécessaire, et même il sera vu que rapidement un accès administratif à ces même données va être organisé pour prévenir toute atteinte à l'ordre public dans le cadre de la lutte contre le terrorisme. Il est du ressort de la puissance publique de pouvoir identifier tout citoyen dans le cadre des opérations de police judiciaire mais également de police administrative. Cette identification doit toutefois être soumise à des conditions strictes pour que ne soit pas porté atteinte aux droits fondamentaux de la personne.

347. **La problématique de l'accès à de telles données dans le cas « poursuites civiles ».** En revanche il faut affirmer qu'un simple particulier ne peut considérer la localisation du point d'accès utilisé par un internaute en dehors de la mise en œuvre de cette action publique. Or le contentieux de la lutte contre le téléchargement illégal va brouiller les frontières des conditions d'accès au fichier de l'article L34-1

La problématique apparaît : un particulier dans le cadre d'une simple requête auprès d'un juge peut-il obtenir à partir d'une adresse IP visible sur le réseau les coordonnées physiques du point d'accès associé à cette adresse auprès du FAI et considérer dès lors les coordonnées de l'abonné et envisager l'identité de l'internaute connecté. Il sera vu que des ayants-droits représentés par leurs conseils souhaitaient obtenir les coordonnées de l'abonné à l'origine d'un téléchargement ou d'une mise en ligne pour le contraindre à un dédommagement en se gardant la possibilité d'agir en justice par la suite. Sur requête ou en référé, le juge a fait droit à leurs demandes. Or cette levée de l'anonymat dans le cadre de poursuites civiles ne peut être.

Cette problématique est aujourd'hui moins présente alors qu'une procédure spéciale a été mise en œuvre dans le cadre des pouvoirs de la HADOPI pour localiser les accès non sécurisés.

348. ***Plan.*** Il convient toutefois d'affirmer clairement que le recours au juge judiciaire est insuffisant pour garantir le respect des libertés individuelles alors que le contrôle de l'identité de l'internaute ne peut ressortir que des pouvoirs de la puissance publique légalement encadrés. Ainsi il faut considérer que la localisation d'un point d'accès ne peut être révélée que dans le cadre de poursuites pénales **(§1)** ou en application d'un régime de réquisition administrative **(§2).**

§1) La nécessaire mise en œuvre de poursuites pénales

349. **La nécessaire mise en œuvre de poursuites pénales.** Le raisonnement ici tenu est le même que s'agissant de la compétence du juge judiciaire à l'égard de la mise en œuvre de mesures de blocage. Le recours au juge judiciaire pour obtenir la localisation du point d'accès ne garantit pas à lui seul le respect de la liberté individuelle de l'internaute. Alors que l'enjeu est ici celui de la levée de l'anonymat, il convient de considérer qu'il intervient comme le « gardien » de celle-ci, devant parer à toute dérive de la puissance publique à cet endroit, seule à même de décider de cette identification.

De la même manière que l'ont montré les décisions visant les mesures de blocage, il sera vu que la jurisprudence cherchant à considérer les conditions de la mise

en œuvre de la divulgation des coordonnées de l'abonné dans le cadre de procédures civiles n'est pas opérante. La mise en œuvre systématique d'un contrôle de conventionalité à l'échelle de mesures préliminaires, nécessitant donc une appréciation de la proportionnalité des mesures demandées, au regard des différents intérêts en présence, ne peut être[685].

350. **La problématique de la surveillance des réseaux P2P avant l'institutionnalisation de procédés de lutte efficace.** Il convient ici à nouveau de s'extraire du contexte de la lutte contre le téléchargement illégal alors que la problématique de l'accès aux données détenues par les FAI s'est cristallisée dans le cadre de celle-ci avant que des procédures adéquates de lutte aient été mises en œuvre avec l'adoption en France notamment de la loi HADOPI.

En effet l'enjeu n'était pas tant de pouvoir identifier les internautes mais de pouvoir interagir avec eux pour les avertir de la surveillance mise en œuvre et d'éventuelles poursuites pénales. Toutefois de fait devant l'ampleur du phénomène il était difficile pour les auteurs et leurs conseils de considérer ces poursuites à l'échelle de milliers de téléchargements ; ainsi la tentation fût d'obtenir les coordonnées de l'internaute dans le cadre de procédures de référés à l'encontre des FAI, pour négocier avec leurs abonnés un dédommagement.

Or cette justice privée ne peut être. Ces cas d'espèce ont révélé la nécessité d'une déjudiciarisation de la répression de la pratique du téléchargement illégal. Elle sera mise en œuvre en 2009 avec la création de la HADOPI et l'encadrement strict d'une procédure dite de « *riposte graduée* »[686].

351. ***Plan.*** Ainsi les procédures de référé visant l'accès aux données détenues par les FAI en application de l'article L34-1 et mises en œuvre dans le cadre de la lutte contre le téléchargement illégal font débat **(A).** Alors qu'à l'époque n'étaient pas encore institutionnalisées des procédures de lutte efficace contre celui-ci, l'insuffisance du recours au juge judiciaire pour lever l'anonymat de l'internaute n'a pas été parfaitement saisi par les commentateurs **(B).**

A] Le débat s'agissant de l'accès aux données de l'article 34-1 dans le cadre de poursuites civiles

[685] V. *supra* 1ère partie, Titre II, Chapitre 1er, Section I, §2, B] « *La nature administrative des mesures à mettre en œuvre* ».

[686] Le Conseil constitutionnel énonce ainsi que l'attribution d'un pouvoir de sanctions à la HADOPI « dans la limite nécessaire à l'accomplissement de sa mission, ne porte pas atteinte à la séparation des pouvoirs ». v. : Décision n°2009-580DC du 10 juin 2009, Loi favorisant la diffusion et la protection de la création sur internet, JORF du 13 juin 2009, p.9675, cons. 14.

352. ***Plan.*** En France, l'affaire dite « *Techland* » révèle les dangers de la procédure de référé pour obtenir les coordonnées de l'abonné et du point d'accès utilisé **(1).** Appelée à se prononcer dans l'arrêt « *Promusicae* », le juge européen ne tranche pas sur le point de savoir si cette divulgation peut avoir lieu dans le cadre de poursuites civiles **(2).**

1) La position du juge français : l'affaire dite « Techland »

353. **L'affaire « Techland » en 2007 : la transmission sur requête des coordonnées de l'abonné à partir de son adresse IP**. En 2007 la société *Techland,* éditrice du jeu-vidéo « *Call of Juarez* » fait appel à la société *Logistep* pour qu'elle mette en œuvre techniquement le relevé des milliers d'adresses IP qui, sur différents réseaux de P2P, se livrent au téléchargement illégal de celui-ci. L'éditeur saisit ensuite le juge sur le fondement de l'article 145 du CPC visant les « mesures d'instruction *in futurum* » pour qu'il requiert des fournisseurs d'accès les coordonnées des abonnés associés à ces adresses. Le juge par trois ordonnances sur requête autorise la société *Techland* à se faire communiquer ces données[687]. Un FAI, *free,* transmet les noms et adresses de ses abonnés concernés.

L'éditeur par l'intermédiaire de son avocat leur fait alors parvenir une lettre de mise en demeure avec accusé de réception qui après avoir détaillé les possibles conséquences d'une assignation en contrefaçon et notamment son coût pour le défendeur, leur propose de régler la somme de 400 euros. Un formulaire de paiement est joint ainsi qu'une attestation à compléter par le supposé contrefacteur qui s'engage à ne pas mettre en partage le jeu vidéo, à effacer toutes les copies qu'il aurait pu conserver et à payer le montant précité. Il n'est précisé à aucun moment que le règlement de cette somme empêcherait les poursuites[688].

De fait devant l'impossibilité de collectiviser les poursuites à l'échelle de 3591 téléchargements relevés, l'idée est d'obtenir réparation par un autre biais. Toutefois ces lettres comminatoires font grand bruit[689].

354. **L'ordonnance de référé-rétractation du TGI de Paris du 25 juin 2007**. Par ailleurs tous les FAI n'entendent pas se soumettre à la requête du juge et agissent en référé rétractation. Ils soutiennent entre autres arguments qu'ils ne peuvent fournir ces données qu'en application de l'article L34-1 du CPCE qui vise la recherche d'infractions pénales. Le TGI de Paris dans son ordonnance du 25 juin 2007 fait droit à leur demande en concluant

[687] TGI PARIS, Ordonnances des 22 janvier 2007, 5 mars 2007 et 30 avril 2007.

[688] V. : FANTI S., *Alcatraz Numérique,* Vevey, Suisse : éd. Xénia, 2009, p.92-97 ; v. également l'article mis en ligne sur le site Legalis.net le 16 avril 2007.

[689] Certains internautes ont même informé le barreau de Paris qui a diligenté une enquête.

qu'il est nécessaire ici qu'une procédure spéciale permettant le contradictoire soit mise en œuvre, soit dans le cas du référé spécial de l'article 6.I.8 de la LCEN, soit dans le cadre de celui de l'article L336-1 du CPI[690].

L'argumentation est peu claire alors qu'il est difficile de considérer en quoi la levée de l'anonymat ou non de l'internaute ressort de l'argumentation des FAI et dans quelle mesure l'identification de l'internaute renvoie à une « *mesures nécessaires à la protection de ce droit et conformes à l'état de l'art* » selon l'article L336-1 ou permette de « *prévenir un dommage ou de faire cesser un dommage occasionné par le contenu d'un service de communication en ligne*» selon l'article 6.I.8 de la LCEN, alors qu'un réseau est visé et que le téléchargement a déjà eu lieu. Cependant cette rétractation décidée, la société *Techland* saisit à nouveau le juge des référés mais cette fois donc, sur le fondement de l'article L336-1 du CPI.

355. **La position du TGI de Paris dans son ordonnance de référé du 24 décembre 2007.** Le juge Emmanuel Binoche dans son ordonnance de référé du 24 décembre 2007 ne fait pas droit à la demande de la société *Techland*[691]. Il est jugé que le traitement d'adresses IP opéré est un traitement de données à caractère personnel illégal alors qu'il n'a pas été soumis aux prescriptions de la loi Informatique et Libertés ; dès lors la mesure d'instruction demandée ne peut être considérée comme légalement admissible. Le juge précise notamment « *qu'enfin , alors que la société Techland ne précise pas ses intentions quant à la saisine de la juridiction civile ou pénale, c'est à elle-même qu'elle demande que soit assurée la transmission de ces données identifiant les internautes* ».

La problématique est absorbée dans celle de la qualification de l'adresse IP en tant que donnée à caractère personnel, toutefois le raisonnement apparait qui veut qu'un ayant-droit ne puisse en dehors d'une action contentieuse accéder aux éléments de l'identité de l'internaute connecté. Quand bien même une infraction est constatée, un particulier ne peut sur simple requête d'un juge judiciaire considérer les coordonnées du point d'accès utilisé et de l'abonnement associé.

Le juge italien en juillet 2007 a lui considéré, dans cette même affaire *Techland* visant un FAI italien[692] que les données ne peuvent être transmises que dans le cadre de

[690] TGI Paris, ord. réf., 25 juin 2007, Neuf Cegetel et autres / Techland, disponible sur le site legalis.net.

[691] TGI Paris, ord. réf., 24 déc. 2007, Techland/ France Telecom et autres, disponible sur le site legalis.net.

[692] Tr. Roma Sez. IX civile-Ord. 14 luglio 2007, *Techland, Peppermint Jam records GmbH /Wind telecommunicazioni* (Tribunale Ordinario di Roma, Sezione IX civile, Specializzata in materia di propriétà industriale e intellectuale).

V. également la communication sur cette décision de la CNIL italienne, la « Garante per la protezione dei dati personali » : « Peer-to-peer : illecito « spiare » gli utenti che scambiano file musicali e giochi (Peppermint)-28 febbraio 2008 », disponible sur le site de l'autorité italienne, www.garanteprivacy.it

la recherche, de la prévention et de la répression de délits pénaux particulièrement graves. Aux États-Unis, en 2003, la Cour d'appel fédérale du circuit du district de Columbia avait quant à elle conclu que l'opérateur de communications électroniques *Verizon* ne pouvait divulguer les coordonnées de ses abonnés dont les adresses IP avaient été relevées sur le logiciel de P2P *Kazaa* en dehors de tout dépôt de plainte, la section 512 *(h)* du DMCA (*Digital Millenium Copyright Act)*[693] ne pouvant s'appliquer au FAI agissant en l'espèce comme un simple conduit des connexions mises en œuvre[694].

Ainsi des incertitudes subsistent : le juge français visant l'action contentieuse, l'on s'interroge sur la possibilité de savoir si dans le cadre d'un litige au fond l'anonymat de l'internaute connecté peut être levé dans le cadre de poursuites civiles. Le juge européen saisi d'une question préjudicielle ne tranche pas la question des conditions de l'accès aux coordonnées du point d'accès utilisé alors qu'il n'exclut pas que ceux-ci puissent être transmis dans le cadre de poursuites civiles laissant cela au choix des États.

2) L'absence de position du juge européen : l'arrêt « Promusicae » du 29 janvier 2008

356. **Les faits de l'arrêt « *Promusicae* » du 29 janvier 2008.** Les faits de l'arrêt « *Promusicae* »[695] sont sensiblement les mêmes que ceux de l'affaire *Techland.* Une société à but non lucratif de producteurs espagnols relève sur un réseau de P2P des adresses IP à l'origine d'actes de contrefaçon et souhaite obtenir du FAI, *Telefonica,* l'adresse physique et l'identité de ses clients associés à de telles adresses. Or l'opérateur de communications électroniques forme opposition contre l'ordonnance l'enjoignant à communiquer de telles données arguant que la loi espagnole n'autorise cette divulgation « *que dans le cadre d'une enquête pénale ou en vue de la sauvegarde de la sécurité publique et de la défense nationale* ».

Dans ces conditions le juge madrilène décide de surseoir à statuer et saisit la CJUE d'une question préjudicielle. Il demande en substance si les directives visant

[693] Cette section permet à un auxiliaire de justice d'une cour fédérale de délivrer une injonction requérant d'un fournisseur de service de communication (*service provider)* qu'il dévoile des éléments d'identification d'un contrefacteur présumé.

[694] GAUBIAC Y., "Logiciels de distribution de musique peer-to-peer. Affaire RIAA c/ Verizon », *CCE,* mars 2004, p. 11. La RIAA (*Recording Industry Association of America*) association américaine qui regroupe les majors de l'industrie musicale a du alors déposé plaintes contre 532 internaute dits « John Doe » (du nom de substitution utilisé dans les actes de procédure en cas de personne dont l'identité n'est pas connue) ; c'est seulement dans le cadre de cette action que le juge pourra ordonner au FAI de fournir les coordonnées des abonnés.

[695] CJCE (aff. C-275/06) Promusicae c/ Téléfonica de Espana Sau.

d'une part le commerce électronique et d'autre part la protection du droit d'auteur[696], lues à la lumière des articles 17 et 47 de la Charte des droits fondamentaux, doivent être interprétées en ce sens qu'elles imposent aux États membres, en vue d'assurer la protection du droit d'auteur, l'obligation de communiquer les données personnelles associées aux données de trafic dans le cadre d'une procédure civile.

357. **L'absence de prise de position du juge européen.** Le juge européen pose ainsi la problématique : il s'agit de savoir si la législation européenne qui ne prévoit pas la communication des coordonnées de l'abonné dans le cadre d'une procédure civile[697], ménageant en cela la protection des données personnelles des internautes et leur droit fondamental au respect de leur vie privée, ne méconnait pas pour autant la protection du droit d'auteur et les droits fondamentaux de propriété et de recours effectif des ayants-droit.

Le juge répond ainsi que la législation européenne visant le droit d'auteur n'impose pas aux États membres de prévoir cette obligation de communication de données personnelles en vue d'assurer la protection effective du droit d'auteur dans le cadre d'une procédure civile. Elle précise cependant, que « *Toutefois, le droit communautaire exige desdits États que, lors de la transposition de ces directives, ils veillent à se fonder sur une interprétation de celles-ci qui permette d'assurer un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. Ensuite, lors de la mise en œuvre des mesures de transposition desdites directives, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'un manière conforme à ces mêmes directives, mais également de ne pas fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité* »[698].

Les images sont nombreuses pour critiquer le raisonnement de la CJUE : on peut lire ainsi que « *le droit communautaire observe une neutralité tout helvétique sur cette question pourtant sensible* »[699], que « *la réponse apportée par la CJCE à cette délicate question s'avèrera être une réponse de Normand* »[700]. Ainsi le juge européen ne

[696] V. les directives : Directive 2000/31/CE, Directive 2001/29/CE, Directive 2004/48.
[697] Directive 2002/58/CE, dite directive « vie privée et communications électroniques », paragraphe 15.
[698] V. le dispositif de l'arrêt.
[699] CARON C., « La communication de données personnelles dans le cadre d'une procédure civile à l'aune du droit communautaire », *CCE*, mars 2008, commentaires n°32, p. 25.
[700] SZUSKIN L., DE GUILLENCHMIDT M, « L'arrêt « Promusicae » : beaucoup de bruit pour rien ? », *RLDI*, avril 2008, actualités, n°37.

tranche pas[701] ce qui est unanimement critiqué mais diversement alors que les enjeux en présence crispent les positions de chacun.

B] L'insuffisance du recours au juge judiciaire

358. ***Plan.*** Tout comme dans le cadre de la problématique de la coupure d'accès au réseau, ce contentieux fait apparaître un vif débat alors qu'il semble qu'on ne peut être pour la défense des droits d'auteur tout en arguant que les coordonnées d'un point d'accès et d'un abonné ne peuvent être communiquées que dans le cadre d'une procédure pénale, et plus généralement à l'instigation des pouvoirs publics.

Or le raisonnement des « défenseurs du droit d'auteur », pour employer à regret une formulation maladroite, est critiquable en ce que l'enjeu de la levée de l'anonymat de l'internaute et le rôle du juge judiciaire à cet égard sont imparfaitement saisis **(1).** De manière plus pragmatique le professeur Caron s'interroge sur l'absence de solution s'agissant de la lutte contre l'usage des réseaux P2P à des fins de contrefaçons en mentionnant la possibilité qu'ont les ayants-droit dans le cadre de services de communication en ligne de se voir communiquer les coordonnées détenues par le FAI sur le fondement de l'article 6.II de la LCEN, dispositions dont la maladresse structurelle apparaît toutefois à cet endroit **(2)**.

1) L'enjeu de la levée de l'anonymat imparfaitement saisi

359. **La critique de l'absence d'effectivité vis-à-vis de la défense du droit d'auteur**. Certains auteurs critiquent vivement l'absence de solution au regard de la défense du droit fondamental de propriété de l'auteur d'une œuvre. Dans un article intitulé « La balance sans l'épée : le droit fondamental sans effectivité», l'avocate Justine Lesueur affirme que « *De surcroît, à quoi sert de rappeler la valeur fondamentale du droit d'auteur si le titulaire des droits ne peut se protéger contre le vol de ses biens»*[702]. Une position tranchée qui doit être nuancée : la voie pénale est ouverte aux ayants-droit.

Le professeur Pollaud-Dulliand[703], pour sa part, condamne la décision et les conclusions plus tranchées de l'avocate générale Juliane Kokott qui affirme que l'exclusion de la divulgation des coordonnées dans le cadre de poursuites civiles est compatible avec la législation européenne et que « *rien ne s'oppose à ce que certains droits d'investigation soient réservés aux autorités publiques ou ne soient tout*

[701] En 2009, elle réaffirme sa position dans l'arrêt dit « *LSG* » traitant de la même problématique dans le cadre d'un contentieux allemand. CJCE, ordonnance (8ème ch aff. C-557/07), 19 février 2009, *LSG c/ Tele2 Telecommunication Gmbh.*

[702] .LESUEUR, « La balance sans l'épée : le droit fondamental sans l'effectivité », *Légipresse*, n°250, avril 2008. p.65.

[703] F. POLLAUD-DULLIAND, Chronique de propriété littéraire et artistique, *RTD. Com*, avril/juin 2008, p. 302.

simplement pas disponibles »[704]. Il regrette que l'avocate générale n'envisage la protection du droit d'auteur qu'à travers la lutte contre la piraterie commerciale et le crime organisé[705]. Il affirme que « *pour l'avocat général, certains droits fondamentaux, sont plus fondamentaux que d'autres, quand bien même ils ne sont invoqués que pour entraver la lutte contre des actes illicites* ». Pour lui, « *on aurait pu faire valoir un raisonnement de type « qui peut le plus peut le moins » : en effet, une procédure pénale, qui peut être exercée en matière de contrefaçon, a des conséquences plus graves pour la personne à identifier que la procédure civile »*[706].

Il faut s'opposer à ce raisonnement : la problématique n'est pas celle des conséquences de l'action mais du respect des libertés individuelles de l'internaute qui ne peut être identifié en dehors de poursuites pénales au risque qu'une justice privée s'instaure quand bien même celle-ci ne consisterait au départ qu'en l'envoi d'avertissements par courriers au domicile de l'internaute à l'initiative des seules sociétés d'ayants-droit.

360. **L'absence de considération de la protection de la liberté individuelle.** Dans le prolongement de ces positions, le professeur Emmanuel Derieux, rappelant que le projet de loi HADOPI est attendu, cherche un « *modus vivendi* » qui ne peut être si l'enjeu de la levée de l'anonymat n'est pas saisi. Ainsi il énonce : « *La conciliation de la protection des droits de propriété intellectuelle et des données personnelles, face aux usages de l'internet s'avère fort délicate. Les initiatives privées doivent être rigoureusement encadrées sinon interdites. Par contre, dès lors qu'un juge intervient, est-il très différent qu'il s'agisse d'actions civiles ou pénales ?* »[707]. Une interrogation qui surprend et à laquelle il faut réagir. La différence entre une instance civile et une instance pénale est majeure : dans la seconde le ministère public est partie au procès, ce qui légitime la levée de l'anonymat de l'internaute à l'origine d'une infraction, trouble à l'ordre public qui impose que l'internaute puisse être poursuivi et condamné quand bien même la partie civile retirerait sa plainte.

D'autres auteurs opèrent également ce glissement faisant du juge judiciaire le garant des libertés individuelles dès lors qu'il est saisi, quand bien même dans le cadre de seules poursuites civiles, quand bien même en référé. Est souvent mentionnée la décision du Conseil constitutionnel de 2004, visant la modification de la loi

[704] Citant le considérant 121 des conclusions générales, *Ibid.*, p.305.
[705] *Ibid.*
[706] *Ibid*, p. 304.
[707] E. DERIEUX, « Le droit communautaire n'impose pas que les législations nationales prévoient l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile », *JCP G.*, 2008, n°21, II. 10099.

Informatique et Libertés. S'agissant de la nouvelle formulation de l'article 9 visant les traitements constatant des infractions et la possibilité nouvelle offerte aux sociétés de gestion de droits d'auteur de mettre en œuvre de tels traitements, le Conseil a en effet énoncé d'une part qu'un tel traitement respecte les droits garantis par la Constitution alors que les adresses IP relevées ne pourront acquérir un caractère nominatif qu' «*en vertu de l'article L. 34-1 du code des postes et des communications électroniques, acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire* »[708]. Par ailleurs alors qu' en revanche il censure la disposition permettant qu'un tel traitement puisse être mis en œuvre plus généralement par toute personne morale, il précise que « *cette déclaration d'inconstitutionnalité ne saurait être interprétée comme privant d'effectivité le droit d'exercer un recours juridictionnel dont dispose toute personne physique ou morale s'agissant des infractions dont elle a été victim*e »[709]. Ainsi il est soutenu que cette procédure judiciaire et ce recours juridictionnel renvoient tout à la fois à une procédure pénale ou civile qui nécessairement doit viser en premier lieu l'identification du contrefacteur et la requête des coordonnées de l'abonné[710].

Cependant la logique de la décision n'est alors par comprise. Les juges de la rue Montpensier mentionnent bien l'article L34-1 qui garantit qu'un système relevant automatiquement des adresses IP sur le réseau en nombre respecte les droits et libertés des internautes, qui ne peuvent être identifiés que dans un second temps dans le cadre d'un procès pénal. Cette mise en œuvre d'une action pénale assure le recours effectif de toute personne physique ou morale victime.

361. **Le champ d'application de l'article 6 de la LCEN.** Un auteur s'interroge par ailleurs s'agissant de l'usage du référé spécial de l'article L336-1 du Code de propriété intellectuelle : « *On peut imaginer que les opérations de filtrage comptent au nombre de ces mesures. Mais peut-on faire entrer dans cette catégorie l'accès aux données personnelles des abonnés ? Pour l'instant aucune réponse jurisprudentielle ne nous permet de l'affirmer*.»[711]. La réponse doit être claire : ni le filtrage d'un site, ni l'accès aux coordonnées du point d'accès utilisé ne peut ressortir d'une procédure civile relevant de la seule maîtrise des particuliers.

[708] Cons. Const., déc. n°2004-499 DC du 29 juillet 2004, loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés, JORF du 7 Août 2004, texte 9 sur 92, considérant 13.

[709] *Ibid.*, cons. 14.

[710] V. par exemple : C. FERAL-SHULH, « Cyberdroit, le droit à l'épreuve de l'internet », 6ème éd., Paris : 2010, *Dalloz (*Praxis Dalloz), p. 524.

[711] J. DALEAU, « Droit d'auteur et protection des données à caractère personnel : arrêt rendu par la Cour de justice des Communautés européennes, gde.ch, 29 janvier 2008, n°C-275-06 *D.*,2008, p.480.

Ainsi si le professeur Caron souligne justement que les dispositions de l'article 6.II de la LCEN permettent d'obtenir les coordonnées de l'abonné dans le cadre d'une procédure sur requête[712], il faut à nouveau souligner la maladresse structurelle de telles dispositions.

2) La maladresse structurelle de l'article 6.II de la LCEN

362. **Les dispositions de l'article 6.II de la LCEN.** L'article 6.II enjoint dans son premier alinéa, non seulement les hébergeurs de contenus mais également les opérateurs de communications électroniques à conserver « *les données de nature à permettre l'identification de quiconque a contribué à la création de contenus ou de l'un des contenus dont elles sont prestataires* ». L'alinéa 3 énonce alors que : « *L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa* ». Dès lors par ce biais, en dehors de tout dépôt de plainte, des ayants-droit ont saisi le juge judiciaire pour qu'il requiert les coordonnées des abonnés auprès du FAI, associées aux adresses IP à l'origine du contenu qui ont été enregistrées par l'hébergeur[713].

Le professeur Caron souligne ainsi que « *La voie de la requête est appropriée car elle évite d'obliger le fournisseur d'accès à être partie à la procédure (comme cela serait le cas dans un référé). Il faut tout de même souligner que ce dernier, qui bénéficie d'un principe de neutralité, n'est pas un contrefacteur et qu'il ne doit donc pas être traité comme tel* »[714]. Effectivement le FAI ne saurait être partie à l'instance. Toutefois inversement il faut s'interroger sur le coût financier devant être supporté par les ayants-droit souhaitant obtenir cette corrélation alors qu'à cet endroit l'article R213-1 du Code de procédure pénale ne peut jouer.

Il faut affirmer que la LCEN s'agissant de la divulgation du point d'accès utilisé ne peut venir déborder les prescriptions de l'article L34-1 du CPCE qui conditionne la divulgation du point d'accès à la mise en œuvre d'une opération de police. En effet la levée de l'anonymat de l'internaute ressort du privilège du pouvoir régalien ; l'expression en ligne doit pour sa part être régulée.

---

[712] CARON C., « La communication de données personnelles dans le cadre d'une procédure civile à l'aune du droit communautaire », *CCE*, mars 2008, commentaires n°32, p. 26.

[713] Pour une synthèse de ces décisions v. : CRIQUI G., « La fourniture d'une simple adresse IP est-elle suffisante ? Ou quand l'obligation à la charge de l'hébergeur doit être précisée. », *RLDI*, 05/2009, perspectives-analyse n°49.

[714] *Ibid.*

363. **La nécessaire exclusion des FAI des prescriptions de l'article 6 de la LCEN**. La maladresse de l'article 6 a déjà été soulignée dans la première section alors que le régime de la surveillance des flux de connexion et celui du retrait des contenus doivent être dissociés. Un contenu illicite doit être retiré après une notification adéquate, en revanche un FAI ne peut bloquer un site sur simple requête.

De la même manière il faut dissocier l'enjeu de l'accès aux données associées à l'adresse IP détenues par le FAI qui permettent la localisation du point d'accès au réseau et la découverte de l'identité de l'internaute connecté, de celui de la conservation de données permettant la surveillance des agissements de l'internaute, à savoir l'adresse IP visualisée par le site web à l'origine de la mise en ligne du contenu.

L'article 6. II de la LCEN doit renvoyer seulement à ce deuxième enjeu : pour organiser la surveillance de l'internaute à l'origine d'un contenu et potentiellement son identification, il est nécessaire de conserver l'adresse IP de la connexion qui a opéré la mise en ligne. En effet, cette adresse pourrait ne pas être conservée par le site web ; c'est une donnée technique, elle permet simplement d'établir la connexion au réseau et n'a pas vocation à être enregistrée un fois l'échange d'informations réalisé. Il a été vu de fait que cette conservation est obligatoire depuis l'an 2000 selon un régime qui aujourd'hui doit être clarifié[715].

La logique est ainsi : l'adresse IP à l'origine du contenu doit être tenue à disposition des autorités judiciaires, qui dans le cadre de poursuites pénales uniquement peuvent requérir des FAI qu'ils l'associent au point d'accès utilisé. Par ailleurs le contrôle de l'identité de l'internaute peut être mis en œuvre par les pouvoirs publics dans le cadre d'une réquisition administrative auprès de ces mêmes opérateurs.

§2) Le régime d'une réquisition administrative

364. **Plan.** La rédaction de l'article L34-1 fait apparaître que s'agissant du pouvoir exécutif les données collectées par les opérateurs de communication électroniques et permettant le contrôle de l'identité de l'internaute, peuvent d'une part être mises à disposition d'autorités administratives aux missions spécifiées que sont la mise en œuvre de la riposte graduée et celle visant la sécurité des systèmes d'information relevant de la sécurité et de la défense nationale **(A).** D'autre part, depuis 2006 et la loi de lutte contre le terrorisme, l'article L34-1-1 du CPCE désormais codifié dans le Code de la Sécurité Intérieure organise l'accès de telles

[715] V. *supra*. Section I., §2), B] « *Le régime visant l'obligation de conserver toute adresse IP à l'origine d'une mise en ligne*».

données dans le cadre de la mise en œuvre d'une opération de police administrative visant d'une manière plus générale la lutte contre le terrorisme **(B).**

A] La prérogative d'autorités administratives aux missions spécifiées

365. **Plan.** L'article L34-1 du CPCE énonce que les données peuvent être mises à disposition de la HADOPI **(1)** et de l'Agence Nationale de Sécurité des Système d'Information (ANSSI) **(2).**

1) La localisation d'un point d'accès par la HADOPI

366. **La compétence de la HADOPI.** La loi n°2009-69 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet[716] organise la lutte contre le téléchargement illégal en créant la Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet, ou HADOPI, une autorité administrative indépendante chargée de mettre en œuvre la riposte graduée[717].

Selon l'article L331-24 du CPI, cette commission agit sur la saisine d'agents assermentés et agréés, mais également sur la base d'informations qui lui sont transmises par le procureur de la République. Elle ne peut être saisie de faits remontant à plus de six mois. Ainsi les agents lui transmettent le relevé des adresses IP à l'origine des actes de contrefaçons et peuvent de fait opérer une surveillance des plateformes P2P alors qu'ils ne peuvent pas par eux-mêmes identifier les internautes derrière ces adresses.

De fait la loi en 2009 donne ce pouvoir à la HADOPI en modifiant l'article L34-1 du CPCE[718] : elle peut requérir des opérateurs qu'au regard de ces adresses lui soient fournies les coordonnées de l'abonné.

367. **La mise en œuvre de la riposte graduée.** La logique ici, en effet, qui a été beaucoup débattue, n'est pas celle de l'identification de l'internaute contrefacteur mais de l'avertissement et de la sanction éventuelle du titulaire de l'abonnement qui est tenu de sécuriser son accès[719].

Ainsi une fois informée des coordonnées du titulaire de l'abonnement, la HADOPI va procéder en trois étapes. D'abord elle envoie à l'abonné, par la voie

[716] Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n°0135 du 13 juin 2009, p.9666, texte n°2.

[717] V. CPI, Partie Législative, première partie, Livre III « Dispositions générales relatives au droit d'auteur, aux droits voisins et droit des producteurs de bases de données », Titre III « Prévention, procédures et sanctions », Section 3 « Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet ».

[718] Article 14, Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n°0135 du 13 juin 2009, p.9666, texte n°2.

[719] Cette nouvelle obligation est définie à l'article 336-3 du CPI.

électronique, via la messagerie fournie par son fournisseur d'accès au réseau, un avertissement. En cas de renouvellement de l'infraction dans un délai de 6 mois, un nouvel avertissement est envoyé par voie électronique mais également par LRAR. Dès lors si une nouvelle infraction est constatée, le dossier sera instruit par le collège et la commission des droits de la Haute autorité et transmis le cas échéant au procureur de la République pour que des poursuites soient engagées sur le fondement des articles L335-7 et L335-7-1 du CPI.

2) La localisation d'un point d'accès par l'ANSSI

368. **La compétence de l'ANSSI.** Depuis 2013 et la loi de programmation militaire[720], l'article L34-1 énonce que les données collectées le sont également « *pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition […] de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L2321-1 du code de la défense […] ».*

Ainsi le constat d'une attaque informatique ne permet pas d'une manière générale un accès direct à la localisation du point d'accès et aux données associées détenues par les opérateurs de communications électroniques ; dans le cas d'une attaque subie par un particulier, une plainte doit être déposée pour que les données dans le cadre de l'instance pénale soient communiquées. En revanche, elles doivent être mises à disposition de l'Agence Nationale de Sécurité des Systèmes d'Information (ci-après ANSSI), une agence qui a été créée en 2009 par décret[721]et qui est rattachée au secrétaire général de la défense nationale. (SGDSN), une autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Comme l'énonce l'article L2321-1 du Code de la défense, cette agence participe de la « *stratégie de sécurité nationale et de la politique de défense en matière de sécurité et de défense des systèmes informatiques »*[722]. C'est à ce titre qu'elle est en lien avec les opérateurs de communications électroniques.

[720] Article 24, LOI n° no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (JORF du 19 décembre 2013).

[721] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

L'ANSSI remplace la Direction centrale de la sécurité des systèmes d'information, créée par décret en juillet 2001.

[722] V. le chapitre 1er « Responsabilités », du titre II « Sécurité des systèmes d'information », du livre III « Régimes juridiques de défense d'application permanente », de la partie 2 « Régimes juridiques de défense » du Code de la défense.

369. **La détection des attaques informatiques visant les systèmes d'information « *affectant le potentiel de guerre ou économique, la sécurité ou capacité de survie de la nation* »**. En effet, l'article L2321-2 du Code de la défense développe sa mission première qui est de répondre aux attaques informatiques visant les systèmes d'information « *affectant le potentiel de guerre ou économique, la sécurité ou capacité de survie de la nation* ».

Dès lors comme le précise, l'article L2321-3 : « *les agents de l'autorité nationale de sécurité des systèmes d'information, habilités par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'Etat, peuvent obtenir des opérateurs de communications électroniques, en application du III de l'article L. 34-1 du code des postes et des communications électroniques, l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou l'atteinte de leur système*. », et de fait de considérer la localisation du point d'accès émettant une adresse IP à l'origine d'une menace.

B] Le pouvoir de la police administrative visant la lutte contre le terrorisme

370. **De l'article L34-1-1 du CPCE à l'article L851-1 du Code de la Sécurité Intérieure.** En 2006 la loi de lutte contre le terrorisme[723] crée à la suite de l'article L34-1, un article L34-1-1 qui organise un accès administratif aux données conservées par les opérateurs de communication électroniques en vue de prévenir les actes de terrorisme. En 2013 la loi de programmation militaire codifie cet article dans le Code de la sécurité intérieure récemment créé[724], dans le cadre d'un chapitre intitulé « *Accès administratif aux données de connexion* ». Ce plan est modifié en 2015 par la loi « *relative au renseignement* »[725] qui crée un Livre VIII dans le Code de la sécurité intérieure intitulé « *Du renseignement* » ; les quatre premiers titres de ce livre définissent un régime commun aux techniques de renseignement qui sont détaillées dans le Titre V. Le chapitre 1er de ce titre vise l'accès administratif aux données de connexion et le premier article de celui-ci, l'article 851-1 vise le recueil de données auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L34-1 du CPCE[726].

[723] Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, JORF du 24 janvier 2006, p. 1129.

[724] Le code de la Sécurité Intérieure est crée en 2012 par l'ordonnance n°2012-351 du 12 mars 2012 relative à la partie législative du Code la Sécurité Intérieure.

[725] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF du 26 juillet 2015, texte 2 sur 49.

[726] Ainsi que le recueil auprès des personnes mentionnées aux 1 et 2 du I de l'article 6 de la LCEN, V. à cet endroit *infra : «Section II : Les conditions de la collecte d'une adresse IP circulant sur le réseau/ §2) Le régime de la collecte de toute adresse IP à l'origine d'un contenu »*.

Cet accès à la localisation du point d'accès au réseau à l'origine de la connexion et des données associées à toute adresse IP en dehors de toute procédure judiciaire ne peut être motivé que par un objectif de lutte contre le terrorisme qui vise la prévention des attaques et non leur répression **(1).** Il fait l'objet d'une procédure stricte encadrant aujourd'hui toute technique dite « *de renseignement* » **(2).**

1) Le développement de la police administrative du terrorisme.

371. **Le développement de la « *police administrative du terrorisme* ».** Lors de la promulgation de la loi de 2006, les commentateurs rappellent l'historique de ce « *régime de police administrative du terrorisme* »[727], à l'origine mis en œuvre par la loi de 1986, renforcé dans les années 1995-1996, et développé fortement depuis les attentats du 11 septembre et les lois de sécurité quotidienne et de sécurité intérieure[728] ; et complété donc en 2006 par cette nouvelle loi de lutte contre le terrorisme.

Il est souligné que le régime visant les actes de terrorisme n'est pas une législation d'exception mais s'inscrit dans le droit commun à travers des dispositions dérogatoires qui visent le développement de procédures dites de « *renseignement* » qui doivent permettre d' « *anticiper sur un éventuel attentat afin, le cas échéant, de l'empêcher ou, à tout le moins d'en dissuader les auteurs* »[729].

Certains dénoncent toutefois le développement de cette « *administrativisation* »[730] de la lutte contre le terrorisme, qui semble entretenir « *la confusion entre dispositifs préventifs, destinés à empêcher la commission d'attentats terroristes, et volets répressifs, destinés à identifier et sanctionner leurs auteurs et complices* ». De fait le Conseil constitutionnel est saisi de la loi et il rappelle, en censurant partiellement la disposition visant les réquisitions administratives de données de connexion, l'exigence de séparation des pouvoirs.

372. **La censure partielle du Conseil constitutionnel.** En 2006, le Conseil constitutionnel saisit de la loi visant la lutte contre le terrorisme censure la rédaction de l'article L34-1-1 du CPCE en ce qu'il énonce que les autorités administratives peuvent accéder aux données détenues par les opérateurs de communications électroniques en vue non seulement de prévenir mais également *« de réprimer les actes de terrorisme »*. Il rappelle que : « *les réquisitions de données permises par les nouvelles dispositions constituent des mesures de*

[727] CHRESTIA Ph., « La loi du 23 janvier 2006 relative à la lutte contre le terrorisme, premières observations », *D.* 2006, p.1409 ; WALINE J., *Droit administratif*, 24ème éd., Paris : 2012, DALLOZ (Précis), p. 356.
[728] ROLIN F., SLAMA S., « Les libertés dans l'entonnoir de la législation anti-terroriste », *AJDA*, 2006 p.975.
[729] CHRESTIA Ph.,*op.cit.*
[730] ROLIN F., SLAMA S., *op. cit.*

police purement administrative ; qu'elles ne sont pas placées sous la direction ou la surveillance de l'autorité judiciaire, mais relèvent de la seule responsabilité du pouvoir exécutif ; qu'elles ne peuvent donc avoir d'autre finalité que de préserver l'ordre public et de prévenir les infractions ; que, dès lors, en indiquant qu'elles visent non seulement à prévenir les actes de terrorisme, mais encore à les réprimer, le législateur a méconnu le principe de la séparation des pouvoirs »[731].

Cela censuré, il reprend pour rejeter les arguments des requérants qui considèrent que ce nouveau régime d'accès aux données porte atteinte à la liberté individuelle et à la vie privée des citoyens français, une argumentation désormais classique qui affirme qu'une conciliation doit s'opérer entre la sauvegarde de l'ordre public d'une part et d'autre part l'exercice des libertés individuelles, dont la défense relève concurremment des deux ordres de juridictions[732]. Cette conciliation est efficiente ici alors que la procédure de réquisitions administratives est assortie de « *précautions et limitations* »[733].

2) La procédure encadrant cette opération de « renseignement ».

373. **Le régime codifié du renseignement.** En juillet 2015 la France adopte une loi relative au renseignement dans le but d'affirmer et de pérenniser la politique publique du renseignement qui a évolué au cours des dernières années dans le contexte de la lutte contre le terrorisme et le développement des nouvelles technologies de communication. Parfois qualifiée de « *Patriot Act* » à la française, la loi complète le Code de la sécurité intérieure créé en 2012 d'un livre VIII intitulé « *Du renseignement* » qui s'ouvre par un article L801-1 qui délimite le cadre des opérations de renseignement.

Pour qu'une conciliation s'opère avec le « *respect de la vie privée, dans toutes ses composantes notamment le secret des correspondances, la protection des données personnelles, et l'inviolabilité du domicile* »[734], ces opérations de renseignement doivent être nécessaires aux intérêts fondamentaux de la Nation énoncés par la loi[735] ; elles doivent être soumises à un régime d'autorisation, mises en œuvre par des agents individuellement désignés et habilités et selon une procédure spécifiée et enfin être proportionnées au but poursuivi[736]. Par ailleurs une autorité administrative indépendante est instituée pour les contrôler, la CNCTR pour « Commission Nationale de Contrôle

[731] Décision n°2005-532 DC du 19 janvier 2006, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

[732] BIOY Xavier, *Droits fondamentaux et libertés publiques*, Paris : Montchrestien, Lextenso éditions, 2013 (LMD édition, Collection cours, *dir.* B. Beignier), p.449.

[733] BERNAUD V., GAY L, SEVERINO C., « Droit constitutionnel », *D.* 2007, p.1166 ; LEPAGE A., « Censure partielle de la loi relative à la lutte contre le terrorisme », *CCE*, mai 2006, n°86, p.43.

[734] Article L801-1 du CSI.

[735] V.TITRE Ier : « Dispositions générales », notamment l'article L811-3 du CSI

[736] V. TITRE II : « De la procédure applicable aux techniques de recueil de renseignement soumises à autorisation ».

des Techniques de Renseignement »[737]. Le Conseil d'Etat est l'organe juridictionnel compétent s'agissant des recours visant les décisions prises[738].

L'article 5 de la loi complète le livre VIII par un titre V définissant : « *Les techniques de renseignement soumises à autorisation* ». Le premier chapitre de ce titre vise « *L'accès administratif aux données de connexion* » et s'ouvre sur l'article L851-1 qui avait déjà été codifié par la loi de programmation militaire de 2013. La technique visée est celle de l'accès aux données détenues par les personnes mentionnées aux articles L34-1 et celles mentionnées au 1 et 2 de l'article 6 de la LCEN[739].

374. **Les dispositions de l'article L851-1 du CSI.** A nouveau en 2015, le Conseil constitutionnel est saisi alors que l'on s'inquiète de cette dénomination générale de *« données de connexion* » soumises à réquisitions[740]. Le Conseil constitutionnel rappelle que les données mises à disposition ne peuvent en aucun cas porter sur le contenu des correspondances et le contenu des informations consultées et que dès lors le législateur « *a suffisamment défini les données de connexion »*[741]. Ce terme recouvre de fait les données relatives au trafic détenu par les opérateurs de communications électroniques en application de l'article L34-1 et les données collectées pour identifier tout créateur de contenu détenues par les sites du web en application de l'article 6.II de la LCEN.

Il rappelle par ailleurs que cette technique est mise en œuvre dans des conditions et avec les garanties « *propres à assurer entre, d'une part, le respect de la vie privée des personnes et, d'autre part, la prévention des atteintes à l'ordre public et celles des infractions, une conciliation qui n'est pas manifestement déséquilibrée »*[742].

Les requêtes visant les données détenues par les opérateurs de communications électroniques et les services de communication en ligne sont mises en œuvre par des agents individuellement désignés et habilités. Alors qu'il s'agit ici d'un accès ponctuel, la logique n'est pas celle de la mise en œuvre d'un traitement soumis à autorisation ; les demandes écrites et motivées sont transmises directement à la CNTCR qui doit rendre un avis.

---

[737] V. TITRE III. « De la commission nationale de contrôle des techniques de renseignement ».

[738] V. TITRE IV : « Des recours relatifs à la mise en œuvre de techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État ».

[739] Par ailleurs la loi encadre deux nouvelles techniques. D'une part l'article L851-2 permet désormais d'accéder à ces données en temps réel ; ainsi par exemple les services de renseignement peuvent considérer immédiatement les numéros appelés par un abonné ou les données de localisation de son téléphone portable. D'autre part l'article L851-3 permet d'imposer aux opérateurs de collecter les adresses IP susceptibles de révéler une menace terroriste. V. *supra* : Section I., §1), B] 2) « La mise en œuvre d'une opération de police administrative visant la surveillance de toutes les connexions à un site web «

[740] Conseil constitutionnel, Décision n°2015-713 DC, du 23 juillet 2015 (Loi relative au renseignement).

[741] *Ibid.* cons. n°55

[742] *Ibid.* cons. n°51.

Conclusion Chapitre 1er

375. **La liberté de collecter une adresse IP naviguant sur le web.** L'adresse IP n'est pas l'identifiant d'un individu. Elle ne révèle rien en soi et doit être librement collectée.

En effet elle réalise le lien nécessaire entre les sites du web et les utilisateurs qui se connectent à eux. L'administrateur d'un réseau local ou d'un site web peut légitimement considérer quelle adresse se connecte à ses services et la mémoriser dans ses fichiers journaux pour opérer une surveillance des connexions. Cela relève d'un enjeu de sécurité informatique et de détection de troubles aux conditions générales d'utilisation du service. Disant cela il s'agit effectivement de réaliser un fichier d'infractions mais cette mémorisation d'une donnée chiffrée ne peut en soi être condamnée. Elle renvoie à la mémorisation naturelle dans le monde physique des traits caractéristiques du visage de tout client d'un commerce par les personnes en lien avec lui. La problématique n'est pas celle de la collecte des adresses IP mais de l'accès au fichier permettant leur corrélation avec une indication tangible renvoyant au monde physique, la localisation du point d'accès qui les a émises. Cette divulgation ne peut intervenir que dans le cas de poursuites pénales alors qu'elle permet une investigation efficace s'agissant de l'identité civile de l'internaute connecté.

En revanche, la mise en œuvre d'une telle collecte d'adresses IP naviguant sur le web par les pouvoirs publics doit être soumise à un régime strict alors que les services de renseignement peuvent sur réquisitions administratives considérer le point d'accès qui les a émises. L'article 851-3 du Code de la sécurité intérieure permet ce dispositif de collecte de toutes les adresses IP se connectant à une boucle du réseau définie. Ce dispositif répond du régime général de toute opération de renseignement et ainsi, en étant autorisé, limité et contrôlé, il ne porte pas atteinte aux libertés individuelles.

376. **L'obligation de conserver toute adresse IP à l'origine d'une mise en ligne de contenu ou d'une connexion à un compte-utilisateur.** Par ailleurs, il faut souligner que si la collecte d'une adresse IP se connectant à un sous-réseau ou un site du web relève d'un principe de liberté, il est un régime qui oblige à la mémorisation de celle-ci.

En effet alors que toute personne à l'origine d'un contenu doit pouvoir répondre de celui-ci, il est nécessaire de conserver l'adresse IP à l'origine de la connexion qui a mis en ligne ce contenu. Ce régime légal est mis en œuvre par l'article 6.II de la LCEN

et son décret d'application n° 2011-219. Toutefois il faut clarifier ce régime : la conservation de la seule adresse IP suffit. Elle permet de mettre en œuvre la responsabilité de l'internaute à l'origine de la mise en ligne par le truchement du fichier de données détenues par le FAI. Les sites du web sont libres par ailleurs de requérir des informations personnelles visant à identifier leurs utilisateurs. Celles-ci répondent d'un autre régime qui doit respecter le « *pseudonymat* » de l'internaute qui peut légitimement considérer que ces informations ne soient pas divulguées en dehors de toute procédure contentieuse quand bien même la réquisition est le fait d'un juge.

Les adresses IP collectées sont ainsi tenues à disposition des autorités judiciaire et administrative qui ne peuvent que dans le cadre de poursuites pénales et de réquisitions administratives spécifiquement encadrées, les relier à un point physique de connexion associé aux coordonnées de l'abonné

377. **La mise en œuvre du pouvoir régalien pour connaître le point d'accès utilisé au regard d'une adresse IP.** Il faut en effet affirmer que le contrôle de l'identité de l'internaute ne peut ressortir que du pouvoir régalien.

Si dans le cadre du contexte de la lutte contre le téléchargement illégal via les réseaux P2P, il y a pu avoir des hésitations quant à la possibilité d'obtenir sur simple requête du juge judiciaire les coordonnées de l'abonné en vue, soit de poursuites civiles, soit simplement d'avertissements délivrés par les conseils des auteurs contrefaits, cette position ne peut plus être. D'une part des procédés de lutte efficaces ont été mis en œuvre alors qu'il est apparu que la procédure de sanction devait être déjudiciarisée à l'échelle du phénomène de masse auquel elle entendait s'attaquer. Dès lors, d'autre part, est apparu le véritable enjeu de l'accès aux données visées par l'article L34-1 du CPCE qui permettent le contrôle de l'identité de l'internaute et qui comme l'indique l'article *stricto sensu* ne peuvent être révélées que dans le cadre de poursuites pénales.

Par ailleurs l'article L34-1 énonce que le fichier permettant la localisation du point d'accès utilisé et donc la révélation de l'identité civile de l'internaute connecté, peut également être mis à disposition de deux autorités administratives aux missions spécifiées : la HADOPI pour la mise en œuvre de la riposte graduée et l'ANSSI en charge de la sécurité des systèmes d'information relevant de la sécurité et de la défense nationale. D'autre part, depuis 2006 et la loi de lutte contre le terrorisme, l'article L34-1-1 du CPCE désormais codifié dans le Code de la Sécurité Intérieure à l'article L851-1 organise l'accès de telles données dans le cadre de la mise en œuvre d'une opération de police administrative visant d'une manière plus générale la lutte contre le terrorisme. Si

le développement de cette police administrative a pu être critiqué, l'accès à de telles données répond du régime général de toute opération de renseignement qui garantit le respect des libertés individuelles de l'internaute.

Si les conditions du contrôle de l'identité d'un internaute à partir d'une adresse IP circulant sur le réseau viennent d'être précisées, il ne peut s'agir de considérer en dehors de tout cadre légal les faits et gestes d'un internaute sur le réseau. Il faut définir les conditions du suivi de la navigation d'un internaute connecté au réseau.

Chapitre 2ème. Les conditions du suivi de la navigation de l'internaute

378. **L'enjeu de la protection de l'anonymat de l'internaute**. L'internaute surfe sur le web, il glisse au gré de ses envies d'un site à un autre et chaque choix est matérialisé par une donnée. Il est ainsi possible de visualiser ce qui intéresse l'individu et même finalement de voir ce qui lui vient à l'esprit. Alors que la dématérialisation du réseau permet à chaque idée ou envie de trouver réponse en un clic, c'est le cheminement intérieur des pensées que l'on peut suivre. De fait l'internaute seul derrière son écran éprouve une grande liberté de choix alors que ceux-ci ne l'engagent pas physiquement. Il est plus simple d'aller consulter des sites spécialisés que d'entrer dans un sex-shop, pour prendre un exemple couramment utilisé et parlant.

Il apparaît ici qu'il faille alors protéger cette liberté de choix et le parallèle immédiat peut être fait avec le secret des correspondances qui sanctionne « *l'intrusion dans le for intérieur* » [743] et qui se prolonge avec l'apparition de la télématique dans l'affirmation d'un « *secret des choix faits parmi les services de télécommunications et parmi les programmes offerts par ceux-ci* »[744]. Toutefois l'enjeu ici de l'atteinte à la liberté individuelle doit être saisi alors qu'il ne s'agit pas d'appréhender un nouveau support fonctionnel[745] de protection eu égard aux données collectées mais bien de définir d'abord un objectif de protection visant l'individu, qui permette de délimiter dans un second temps l'objet à protéger.

Il a été vu que l'internaute doit pouvoir accéder librement au réseau en ce sens qu'il doit lui être garanti qu'il ne peut être identifié à son insu. La protection de la navigation n'a pas à porter sur n'importe quelle donnée indiquant une information consultée mais bien sur l'ensemble des faits et gestes d'un internaute qui peuvent renseigner sur son identité réelle.

379. ***Plan.*** L'état des lieux de la législation actuelle visant la collecte des données révélant les informations consultées fait apparaître que l'objectif de respect de l'anonymat de

[743] V. BONAN F., « Violation du secret des correspondances par un particulier », *JurisPTT*, n°15, 1er trimestre 1989, p.35

[744] LOI n°86-1067 du 30 septembre 1986 relative à la liberté de communication (dite loi Léotard), article 3.

[745] FAVOREU Louis, *et al.*, *Droit des libertés fondamentales*, 6ème éd., Paris : Dalloz (Précis, droit public, science politique), p.264.

l'internaute n'est pas parfaitement réalisée par celle-ci **(Section I)**. Dès lors il faudra réfléchir au contenu d'un nouveau régime visant le secret de la navigation de l'internaute **(Section II).**

Section I. L'état des lieux de la législation applicable aux données révélant les informations consultées

380. **Les traces produites par la technologie numérique**. La nouveauté de la communication numérique est d'être productrice de données. En effet la transmission du message ne se réalise plus de manière analogique par la variation d'un phénomène physique comme une modulation du courant électrique, une modulation des ondes de la lumière ou une modulation d'une onde hertzienne[746], la communication est traduite en une suite de nombres.

Dès lors il n'est plus nécessaire de mettre en œuvre un procédé technique permettant de décompter les actes de communication comme la mise en place d'un autocommutateur dans le cadre d'une liaison téléphonique. Ces données renseignant sur la fréquence d'utilisation du réseau et sur les sites visités et services utilisés sont produites automatiquement par l'usage de la technologie numérique. Elles révèlent les choix de l'internaute, autrement dit son parcours d'un site vers un autre sur le réseau internet.

Ainsi l'on peut parler de traces, terme qui est défini comme « *un suite d'empreintes laissées sur le sol par le passage de quelqu'un, d'un animal, d'un véhicule* »[747] ; la trace est « laissée », ce qui est involontaire et elle témoigne d'un « passage », un terme qui fait référence aux mouvements de la personne. Ce terme est adéquat pour désigner les données qui permettent la connexion à un réseau de communication. Or de la même manière que la matérialisation du passage d'un animal ou d'un individu peut, dans le monde physique, conduire à son identification[748], sur le réseau internet, le relevé de tous les choix opérés parmi les services et les informations

[746] Les variations du signal initial sont reprises dans les mêmes proportions, c'est-à-dire de façon « analogue » par le phénomène physique qui en assure la transmission. V. : BALLE Francis, *Médias et Sociétés*, 16ème éd., Paris : L.G.D.J Lextenso éditions, 2013, n°174 p.188.

[747] Voir la définition de traces sur le Larousse en ligne : www.larousse.fr

[748] Ainsi le roman « *Le nom de la Rose* » de l'universitaire italien Umberto Eco s'ouvre sur cette scène où le moine Guillaume arrivant à proximité de l'abbaye renseigne très exactement des moines parti à la recherche d'un cheval échappé, sur la direction qu'a pris celui-ci, sur son nom et sur ses qualités, alors même qu'il n'a pas croisé l'animal. A son disciple, qui l'interroge sur cette remarquable sagacité, il répond : « *Mon bon Adso,* -dit le maître-. *J'ai passé tout notre voyage à t'apprendre à reconnaître les traces par lesquelles le monde nous parle comme un grand livre. Alain de Lille disait que, Omnis mundi creatura, Quasi liber et pictura, nobis est in speculum, et il pensait à l'inépuisable réserve de symboles avec quoi Dieu, à travers ses créatures, nous parle de la vie éternelle. Mais l'univers est encore plus loquace que ne le pensait Alain, et non seulement il parle des choses dernières (en ce cas-là, il le fait d'une manière obscure) mais aussi des choses proches, et alors là d'une façon lumineuse ».* Guillaume renseigne alors Adso sur les divers indices qui lui ont permis d'aboutir à une juste supposition : la clarté des empreintes des sabots dans la neige, les branches cassées à hauteur d'encolure, les crins de jais retenus par les épines d'un buisson. V. ECO U., *Le nom de la Rose,* Paris : Grasset, 1982.

à disposition peut conduire à identifier la personne derrière son ordinateur. Dès lors, il faut prohiber cette identification automatique, à l'insu de la personne, qui se réaliserait à partir de l'exploitation des données révélant sa navigation sur la toile.

381. ***Plan***. Toutefois il faut constater d'une part que la mise en œuvre d'un tel objectif apparaît très maladroitement dans le régime actuel visant la confidentialité des communications électroniques **(§1).** D'autre part il sera vu que l'encadrement de la mise en œuvre d'un cookie qui n'est pas envisagé au regard de cet objectif apparaît inadéquat s'agissant de la protection des libertés individuelles de l'internaute **(§2).**

§1) La maladresse du régime visant la confidentialité des communications électroniques

382. **L'évolution des secrets dits « de communication ».** Les secrets dits « de communication » protègent les choix relatifs à la mise en relation souhaitée dans le cadre d'une communication à distance. Au-delà de la protection du contenu échangé, ils visent à permettre la libre utilisation du moyen de communication mis à disposition. L'individu doit être sur que la manière dont il l'utilise ne peut faire l'objet d'un suivi.

Ainsi il faut noter que la jurisprudence a reconnu très tôt que le secret des correspondances visait également le choix des destinataires de celle-ci**.** Plus tard il a été affirmé que celui-ci condamnait également la mise en place d'un système de comptage des appels opérés depuis une ligne téléphonique. Puis avec l'essor de la télévision, nouveau média de masse, et le développement de la télématique il a été consacré dans la loi française un secret des choix faits par les usagers parmi les programmes qu'ils peuvent recevoir.

Toutefois la numérisation de la communication au tournant du XXIème siècle va opérer une dilution contestable des objectifs visés. Alors que l'accent est mis sur la production automatique de données qui se multiplient, l'objectif de la protection visant l'acte de communication se dilue au profit d'une protection des données produites d'une manière générale par la communication dont la collecte ne doit pas porter atteinte à la vie privée.

383. ***Plan*.** L'historique de la protection des choix de communication **(A)** permet de considérer qu'un coup d'arrêt a été porté à l'évolution de ce régime avec l'affirmation d'un principe d'effacement des données relatives au trafic **(B)**.

A] L'historique de la protection des choix de communication

384. **Plan**. Il convient de rappeler que la problématique des choix de connexions, qui ne consistent pas en des contenus est ancienne. Ainsi on s'interrogeait déjà sur la divulgation de l'émetteur et du destinataire d'une lettre et sur celle des numéros de téléphone appelés. Il est constant aujourd'hui que ces informations sont couvertes par le secret des correspondances et leur divulgation obéit donc au régime légal des interceptions de communication. **(1)** Eu égard à l'atteinte qui pourrait être faite à la liberté de communication, alors qu'un service interactif révèle les goûts et autres centres d'intérêts d'un utilisateur, un secret spécifique des choix des programmes de la communication audiovisuelle, est énoncé en 1982 qui trouvera à se prolonger avec l'apparition des services télématiques **(2).**

1) Le secret du choix des destinataires d'une communication

385. **Le secret de l'indication de l'expéditeur et du destinataire d'une lettre.** Dans un arrêt de 1903, la Cour de cassation, en sa chambre criminelle[749], dans une affaire où il était demandé aux employés des postes l'identité d'un homme qui venait retirer certaines lettres, affirme que le serment professionnel des préposés de l'administration des postes couvre non seulement le contenu des correspondances mais également les noms des expéditeurs ou des destinataires des lettres qui leur sont confiées. Ils ne peuvent révéler ceux-ci que dans le cadre d'une instruction ou instance criminelle ou correctionnelle. Cette position fait débat.

Le conseiller Dumas, dans son rapport à la Cour, ne considère pas qu'une adresse puisse faire l'objet d'un secret alors qu'elle est nécessairement exposée aux yeux de plusieurs personnes, celles qui attendent au guichet de la poste ou encore la concierge qui peut garder plusieurs jours la lettre dans sa loge. Un juge d'instruction au tribunal de la Seine lui répond que le secret doit s'étendre à ces informations alors qu' « *il peut, en effet, y avoir les plus graves inconvénients pour une personne à ce que l'on sache que tel jour, il est arrivé à son adresse une lettre venant de telle destination* » et il souhaite que l'on donne « *à la règle du secret un caractère plus absolu* »[750].

En réalité, l'incidence sur la vie privée de l'individu dépend de la concentration des informations aux mains d'une personne, en l'occurrence ici le fonctionnaire des postes. Il est à même de connaître l'ensemble des destinataires d'un individu et la fréquence de ses échanges et l'on ne peut alors qu'aller dans le sens de la Cour de cassation, en incluant ces informations dans le secret des correspondances. Un

[749] Cass. Crim., 5 novembre 1903, *DP* 1904 I. 25, note Le Poittevin.
[750] *Ibid*, p.28.

guichetier ou un facteur ne peut révéler au public que Mme Labelle vient, tous les jours, retirer une lettre envoyée par M. Dupont[751].

386. **Le secret des numéros de téléphone composés**. Cette même problématique s'est posée quant à la divulgation des numéros appelés à partir d'un poste téléphonique. En 1991, un avocat conteste la facture de son poste de téléphone professionnel et en demande le détail auprès de l'administration des PTT. Celle-ci consent à le lui communiquer, en occultant toutefois les quatre derniers chiffres des numéros appelés, ce dont l'abonné ne se satisfait pas. L'affaire est portée devant le Conseil d'Etat qui, dans son arrêt Burki[752], confirme le rejet de la demande de l'avocat par la Cour administrative d'appel de Lyon, considérant que « *la communication d'une copie des numéros d'appel complets permettrait au titulaire de connaître l'identité des personnes appelées par des tiers utilisant le même poste ; que cette communication porterait atteinte au secret de la vie privée des tiers et de leurs interlocuteurs* ».

Les conclusions du commissaire du gouvernement[753], qui ont été suivies, sont limpides alors qu'il est « *résolument partisan d'un défense stricte du secret* » qui protégerait le numéro de téléphone appelé et, par conséquent, le nom du correspondant au même titre que le contenu même de la communication. A l'argument qui voudrait que l'abonné qui paie les communications soit en mesure de connaître les appels téléphoniques, une exigence légitime dans le cas d'une entreprise, il oppose la nécessité d'informer la personne du procédé de surveillance. L'intime ne pouvant être surpris qu'à l'insu du salarié, il indique que l'enregistrement alors ne « *violerait plus aucun secret, ou du moins aucun secret devant être protégé. Ceux qui violeraient la règle interne de l'utilisation de la ligne téléphonique familiale ou professionnelle se placeraient en quelque sorte hors la loi et on leur appliquerait l'adage Nemo auditur propriam turpitudinem allegans* ».

[751] Le Doyen Gény souligne ainsi dans son ouvrage sur les lettres missives de 1911 « *L'agent des Postes ne doit, dans sa manipulation des correspondances, prendre aucune connaissance de ce qu'elles renferment ; il ne doit même en considérer les apparences extérieures (origine, adresse, etc.) qu'en vue d'en exécuter son service à leur égard, et notamment de les acheminer vers leur destination. […] l'agent des Postes ne doit rien divulguer, ni communiquer à personne. Il doit même s'abstenir rigoureusement de faire connaître, soit l'existence d'une correspondance (ou de tout autre opération du service postal, télégraphique ou téléphonique), soit les circonstances de lieu, de temps, de personnes (nom, domicile, profession des correspondants), ou autres, qui en auraient accompagné la remise, le transport ou la distribution* ». V. *Des droits sur les lettres missives, étudiés principalement en vue du système postal français*, Recueil Sirey : Paris, 1911, p. 79 et 80.

[752] CE, 6 février 1991, *Burki*, Req.n°49663, *Recueil Lebon* 1991, p.39

[753] Conclusions de Bernard de Froment, commissaire du gouvernement, *AJDA*, 20 juin 1991, jurisprudence p.467.

387. **La position de la Cour européenne des droits de l'homme quant au détail des numéros de téléphone composés**. Dans l'arrêt Malone du 2 août 1984, la CEDH[754] est amenée à prendre position sur un procédé de « comptage » (metering en anglais), qui enregistre les numéros formés sur un téléphone donné ainsi que l'heure et la durée de chaque appel. Le Post office britannique l'a conçu pour son propre usage ; ce procédé lui permettant de veiller à l'exactitude du montant des redevances demandées à l'abonné. M. Malone se prévaut devant la cour d'une atteinte à l'article 8 de la Convention protégeant la vie privée et familiale, le domicile et la correspondance. Il suppute, en effet, qu'un tel relevé à été transmis à la police, en dehors de tout cadre légal, alors que ce détail des appels d'un abonné ne peut être communiqué que sur injonction d'un juge dans le cadre d'un procès.

Le gouvernement britannique tente de faire valoir qu'à la différence de l'interception des communications, le comptage ne porte pas atteinte à l'article 8 de la Convention. Un argument rejeté par la Cour de Strasbourg, qui indique qu'elle « *ne considère pas pour autant que l'exploitation des éléments rassemblés de la sorte ne puisse jamais poser de problème sur le terrain de l'article 8 (art. 8). Dans un relevé ainsi dressé figurent des informations - notamment les numéros composés - qui font partie intégrante des communications téléphoniques. Aux yeux de la Cour, les révéler à la police sans l'accord de l'abonné porte donc aussi atteinte à un droit consacré par l'article 8 (art. 8).* ». La formulation de la Cour est à saluer, dès lors qu'elle semble souligner les évolutions à venir et qu'elle inclut logiquement le choix des correspondants dans la sphère d'intimité qui doit être réservée à tout individu.

388. **L'évident secret des choix de services dans le cas d'une communication interactive**. Si le choix des correspondants tombe sous le coup du secret des correspondances, qui garantit le respect de la vie privée, il ne peut en aller autrement des choix de services lorsqu'un nouveau moyen de communication et de diffusion de l'information apparaît : le minitel. A l'époque l'opérateur technique est unique et le réseau est national et centralisé : France Télécom connait l'ensemble des services consultés à partir du minitel d'un abonné. Un secret de ces choix est consacré dans la législation française.

2) Le secret du choix des programmes et des services de la télématique

389. P**lan**. Le secret des choix des services de télécommunications et des programmes qu'ils proposent est affirmé dès 1982 puis reformulé dans l'article 3 de la loi de 1986 relative

[754] CEDH, Affaire Malone c/ Royaume-Uni, Req.n°8691/79, du 2 Août 1984.

à la liberté de communication **(a).** La problématique apparaît à l'endroit de son régime alors que la nouveauté du secret rend ses contours encore incertains **(b).**

a. L'énoncé du secret.

390. **1982 : Le secret du choix des programmes**. La loi du 29 juillet 1982 sur la communication audiovisuelle énonce déjà dans son article 3 que «*Sauf accord des intéressés, l'anonymat des choix faits par les usagers parmi les programmes qu'ils peuvent recevoir doit être garanti* »[755]. La loi du 30 septembre 1986 sur la liberté de communication, qui abroge en partie celle de 1982[756], maintient cette prescription dans son article 3[757] : « *Le secret des choix faits parmi les services de télécommunications et parmi les programmes offerts par ceux-ci ne peut être levé sans leur accord* ».

Le terme « programme » qui renvoie à la communication audiovisuelle, démontre déjà qu'un sentiment d'interactivité est né avec la démocratisation de la télévision. Le choix des chaînes et des programmes est propre à chacun et doit être anonyme. Dans les faits, la technique de diffusion audiovisuelle ne permet pas en soi de relever ces choix. Un boitier doit être relié à la télévision pour qu'ils soient enregistrés ; c'est ainsi que se mesure l' « Audimat »[758], qui en vertu de la loi, ne va donc être calculé qu'à partir d'un échantillon de la population qui a consenti à l'installation du boitier et à la levée du secret.

391. **Le secret du choix des services télématiques**. La garantie de secret, issue des lois de 1982 et 1986, se comprend davantage au regard de l'interactivité permise par la télématique. La télématique s'oppose en effet aux médias de masse alors qu'elle n'est pas un moyen de diffusion de l'information mais un moyen de communication de celle-ci. Elle est ainsi définie dans la loi de 1982, à l'article 77, comme un « *service de communication audiovisuelle avec le public en général ou avec des catégories de public par lequel chaque utilisateur du service proposé interroge lui-même à distance un ensemble d'écrits, de sons, d'images ou de documents ou messages audiovisuels de toute nature, et ne reçoit en retour que les éléments demandé* ». La loi de1986 ne reprend malheureusement pas cette définition qui caractérisait justement l'interactivité de la télématique.

[755] LOI **n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle, JORF 30 juillet 1982, p. 2431**

[756] LOI n°86-1067 du 30 septembre 1986 relative à la liberté de communication (dite loi Léotard), JORF du 1 octobre 1986, p. 11755.

[757] Cette prescription est en 1986 prévue à l'article 1er alinéa 3 de la loi sur la liberté de communication ; sa numérotation change après la modification opérée par la loi 89-25 du 17 janvier 1989.

[758] V. MAISL Herbert « La protection des données et des systèmes » *in* HUET Pierre (*dir.*), *Le droit du multimédia, de la télématique à Internet,* Paris : Les éditions du téléphone, 1996. (Rapport de l'AFTEL : association française de la télématique et du multimédia, p.185.

Celle-ci est dans la loi nouvelle, un moyen de télécommunication qui, lorsqu'il n'établit pas un échange de correspondances privées, est un moyen de communication audiovisuelle. Une dénomination maladroite qui se comprend par la nouveauté et l'ambivalence de la télématique qui permet tout à la fois, la communication d'informations et l'échanges de correspondances privées.

Toutefois, si la nature des messages échangés et le secret ou non qui y est attaché, ouvrent une problématique nouvelle qui perdurera dans les premières années du développement d'internet, le secret des demandes des utilisateurs est lui garanti. Ainsi Pierre Huet, conseiller d'Etat, citant l'article 3 de la loi de 1986 indique que « *même si le contenu d'un service relève de la communication audiovisuelle, parce qu'il porte sur des données accessibles au public, l'appel d'un usager garde le caractère d'une correspondance privée et il est à ce titre confidentiel »*[759]. Un autre commentateur souligne cette même logique et conclut alors que « *Dans ces conditions, il n'est pas interdit de penser que la notion de correspondance, qui ne reflète pas totalement la réalité complexe des communications échangées sur les réseaux, peut à terme poser un délicat problème d'interprétation pour les tribunaux. Le secret des correspondances devra sans doute faire place au secret des communications »*[760]. L'enjeu est alors celui de la garantie d'un tel secret.

b. Le régime d'un tel secret

392. **Une déclaration de principe.** Le secret tel que formulé dans les lois de 1982 et 1986 est une déclaration de principe qui ne peut recevoir en tant que tel d'application concrète. En effet, le principe de légalité pénale s'oppose à ce que ce secret soit assorti d'une sanction propre dès lors que les contours de sa violation ne sont pas précisés. Il faut définir qui est concerné par ce secret et en quoi consisterait sa violation. Or les acteurs qui pourraient détenir de telles données ne sont pas identifiés et les données elles-mêmes ne sont pas matériellement définies. La difficulté à l'époque, qui persiste encore aujourd'hui, est que l'enjeu est ressenti mais que sa réalité concrète est peu comprise. Il apparaît à tous que les choix de services doivent rester secrets sans qu'on sache très bien qui les collecte et comment.

Certains arguent de l'application des dispositions pénales du droit spécial des fichiers informatiques et notamment de la sanction des collectes opérées par un moyen

[759] V. HUET Pierre « Les services multimédias » *in* HUET Pierre (*dir.*), *Le droit du multimédia, de la télématique à Internet*, Paris : Les éditions du téléphone, 1996. (Rapport de l'AFTEL : association française de la télématique et du multimédia, n°33 p.53.

[760] AUDIGOU Alain, « La protection pénale des télécommunications », *JurisPTT, la revue du droit des PTT*, n°6, octobre 1986, p.5.

frauduleux ou illicite[761]. Un raisonnement qui apparait spécieux alors que le caractère technique et l'automaticité de la production de traces sur un réseau ne répond pas à la logique de la création d'un fichier. Il faut s'interroger concrètement sur les acteurs de la communication et sur les données qui sont à leur disposition et ce qu'elles révèlent. Or, à l'époque, les choix de services sont centralisés par un seul opérateur, l'opérateur historique et étatisé : France Télécom.

393. **Le rôle de l'opérateur historique France Télécom.** A l'époque de la mise en œuvre du réseau national Transpac et de la diffusion du terminal dédié qui permet d'y accéder, le minitel, le secteur des télécommunications en France n'est pas libéralisé. Un seul opérateur, alors administration d'Etat rattachée au ministère des postes et des télécommunications, contrôle les lignes téléphoniques et leur utilisation : la Direction Générale des Télécommunications (DGT), qui deviendra en 1988, France Télécom.

France Télécom, en situation de monopole, propose d'abord sur ce réseau son propre service d'annuaire le « 36 11 » mais très vite face à la grogne des patrons de presse, décide de libéraliser les services accessibles[762]. La question qui se pose alors est celle de la rémunération de tels services ; est mis en œuvre pour ce faire le système « kiosque ». Le prix des services accessibles via le minitel vient s'ajouter au prix de la communication téléphonique sur la facture reçue par l'abonné. Ainsi, pour avoir accès au réseau, les particuliers ne traitent qu'avec un opérateur, qui met à leur disposition gratuitement le terminal et leur facture l'utilisation de l'infrastructure des lignes téléphoniques, suivant la durée et la nature du service choisi. Ce système kiosque assure le succès du minitel alors qu'il fonde un modèle économique sûr pour les fournisseurs de services, et qu'il permet par ailleurs l'anonymat de l'usager vis-à-vis de ces services alors qu'il n'est pas directement en contact avec eux pour leur facturation[763].

Le secret des choix des services doit alors être gardé par France Télécom, qui est seul à même de détailler les choix des services de son abonné.

---

[761] *Ibid.*

[762] La libéralisation est limitée aux entreprises de presse alors qu'il faut, pour pouvoir créer un service télématique, diriger une société de presse agréée par la Commission des publications et agences de presse. Ce régime d'agrément est cependant vite dévoyé alors que les personnes désirant créer un service télématique, créent pour ce faire des fanzines ou autres journaux quand d'autres sous-louent carrément les agréments de leurs publications. V. le billet sur le blog « A l'œil » de Michel Puech, « Le monde du Minitel se paye Le Monde », article mis en ligne le 20 juin 2010 et racontant comment Claude Perdriel et Xavier Niel ont créé les premiers services lucratifs du Minitel, http://blogs.mediapart.fr/blog/michel-puech.

[763] HUSSON G., « Le Minitel, "faux-frère" d'Internet, ferme définitivement », article mis en ligne le 29 juin 2012 sur le site web du journal Le Monde, rubrique technologies : http://www.lemonde.fr/technologies/ ; HUET J., DREYER E., *Droit de la communication numérique*, Paris : LGDJ Lextenso éditions, 2011 (Manuel), point 56 « Fonction "kiosque" et contrats », p.58.

394. **L'application du secret à la facture détaillée**. Les différents services disponibles via le Minitel, obéissent à une grille de tarification mise en œuvre par le code que l'utilisateur doit taper pour accéder au service. Ainsi, les codes « 3611 », « 3613 », « 3614 » « 3615 » sont facturés de 0,02 à 1,41 euro la minute[764].

Dès lors ces codes et la durée d'utilisation d'un service permettent à France Télécom d'établir la facture de l'abonné. Toutefois pour préserver le secret énoncé dans la loi, et dans la même logique qui veut que la facture détaillée d'un abonné occulte les derniers chiffres d'un numéro appelé, la facture ne précise pas le nom du services télématique demandé[765]. Un abonné visualisera qu'il a consommé, ou qu'une personne de son domicile a consommé, 15 minutes d'un service dont le préfixe est 3615 sans qu'il sache s'il s'agit du 3615 ULLA ou du 3615 Météo France.

Ainsi à l'époque du minitel, les acteurs qui ont accès à la navigation d'un abonné entre les différents services proposés par le minitel se limitent à l'opérateur historique. Soumis au secret des choix et au respect de la vie privée, il ne peut révéler ceux-ci et agit en conséquence quant à la facturation détaillée, qui ne peut faire apparaître les choix de connexions des différentes personnes du foyer.

Or dès 1996, le professeur Maisl s'interroge sur les données collectées par les FAI alors qu'à la différence du minitel et de son système kiosque, la facturation n'est plus dissociée selon les services utilisés : « *Sur des réseaux comme Internet, le fournisseur d'accès détient un fichier de ses abonnés s'acquittant chaque mois, d'une facturation forfaitaire. Celui-ci, a priori, fait donc l'impasse sur le suivi des usages mais il faudrait vérifier s'il en reste des traces, pendant combien de temps celles-ci sont conservées et pour quelles finalités* »[766]. Ce régime procède d'un nouveau principe qui vise la confidentialité des communications électroniques qui renvoie au régime des données relatives au trafic qui toutefois fait difficilement apparaître cette exigence de secret.

B] L'actuel principe d'effacement des données relatives au trafic

395. **La confidentialité des communications électroniques et des données y afférentes**. Dès la fin des années 90 la législation européenne consacre la confidentialité non seulement du contenu des communications mais également des « *données afférentes à celles-ci* » alors

[764] HUSSON G., « Le Minitel, "faux-frère" d'Internet, ferme définitivement », *op. cit.*

[765] NOSSOVITCH Marie-Claire, « Les utilisations délictuelles du kiosque télématique », *JurisPTT*, n°25,1990, p.47

[766] HUET Pierre (*dir.*), *Le droit du multimédia, de la télématique à Internet*, Paris : Les éditions du téléphone, 1996. (Rapport de l'AFTEL : association française de la télématique et du multimédia), contribution de Herbert Maisl « La protection des données et des systèmes », point 56.

que les réseaux sont désormais numériques et qu'une trace de chaque action de communication est désormais produite automatiquement. Révélant tout autant que la communication, ces données dites *« de trafic »* doivent être effacées une fois la communication achevée. Est ainsi consacré le secret des destinataires appelés et celui du comptage des appels qui trouvent à se prolonger dans celui du comptage des connexions au réseau et du choix des applications de communications utilisées, ainsi que des informations consultées et du lieu physique de connexion alors que la communication est désormais mobile.

Toutefois comme il a déjà été souligné, la difficulté est alors que la loi va définir un encadrement qui est fonction d'un type technique de données, les données produites au point d'accès au réseau et non de ce qu'elles révèlent sur l'individu ; les différents objectifs de protection à atteindre ne sont pas dissociés.

396. **La maladresse d'un tel régime.** L'objet de la protection, les données, devient l'objectif de protection puisqu'il semble qu'il faille les protéger en soi. Or le contexte de la lutte contre le terrorisme fait apparaître une logique de surveillance compulsive : à partir du moment où les données existent, il convient de les conserver dans le but de sauvegarder la sécurité publique. La question de l'atteinte aux libertés individuelles n'est alors plus posée qu'en termes de protection des données personnelles conservées.

Ainsi la directive de 2002 dite *« vie privée et communications électroniques »* est modifiée en 2009[767] : la confidentialité concerne désormais également le traitement des données à caractère personnel dans le secteur des communications électroniques. Est définie la « *violation de données à caractère personnel* », qui renvoie à la sécurisation des traitements de données mis en œuvre[768]. Formellement en droit français, l'article L32-1 du CPCE est modifié en 2015[769] : l'objectif de protection des données personnelles à la charge des opérateurs de communications électroniques est placé avant celui du secret des correspondances.

[767] V. Dir. 2009/136/CE, JOUE 18.12.2009, L337/11-36. Le paquet Telecom a en effet été révisé en 2009 par deux directives du 25 novembre 2009 : la directive 2009/140/CE (JOUE 18.12.2009, L337/37-69) qui modifie la directive CADRE, la directive ACCES et la directive AUTORISATION (dite en anglais *« better regulation directive »*), et la directive 2009/136/CE (JOUE 18.12.2009, L337/11-36) qui modifie la directive SERVICE UNIVERSEL et la directive VIE PRIVEE ET COMMUNICATION ELECTRONIQUE (dite en anglais la « *citizens rights directive* »)

[768] V. le nouveau point h) de l'article 2 de la directive 2002/58/CE telle que modifiée en 2009 : « "violation de données à caractère personnel " : *une violation de sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté* ».

[769] Loi n° 2015/990 du 6 Août 2015 pour la croissance, l'activité et l'égalité des chances économiques, article n°120.

397. ***Plan.*** Ainsi il faut constater d'une part le déclin du secret des correspondances **(1)** et d'autre part la faiblesse de l'affirmation du principe de secret des informations consultées sur le réseau **(2)**.

1) Le déclin du secret des correspondances

398. ***Plan.*** Le secret des correspondances est limité par l'approche technique visant désormais des données qui en est faite **(a)** et affaibli par une logique critiquable qui généralise l'exception visant la rétention de ces données **(b).**

a. La limitation du champ d'application du secret

399. **Une protection à la charge des seuls « opérateurs de communications électroniques ».** La législation européenne restreint la portée de la protection en visant spécifiquement les acteurs qui collectent les données relatives au trafic : « *le fournisseur d'un réseau public de communications ou le fournisseur d'un service de communications électroniques accessibles au public* »[770]. Ainsi en application des définitions de la directive cadre est concerné d'une part l'opérateur qui exploite structurellement le réseau et d'autre part l'opérateur qui fournit le service d'accès au réseau auprès des particuliers[771]. Quand bien même ces deux fonctions sont aujourd'hui dissociées et ne font plus l'objet d'un monopole historique, l'approche reste classique[772]. La confidentialité des données relatives au trafic est mise à la charge de l'opérateur de communication, c'est-à-dire celui qui achemine le message via la mise à disposition du réseau physique ou via la mise à disposition d'une connexion au réseau. Ces opérateurs sont identifiés dès lors qu'ils doivent faire l'objet d'une déclaration auprès de l'ARCEP[773].

Or cette délimitation réduit la portée du secret des correspondances alors que la communication numérique est marquée par la convergence. Même si en 2002 au moment de la création de la directive, des services comme *Skype ou whatsapp* n'existaient pas

[770] Directive 2002/58/CE, article 6 « Données relatives au trafic », paragraphe 1.

[771] V. Dir. 2002/21/CE du 7 mars 2002, JOCE 24.04.2004, L108/33-50, article 2) « *Définitions* », a) « *réseau de communication électroniques* », c) « *service de communications électroniques* : *le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les service consistant à fournir des contenus à l'aide de réseaux et de services de communciations électroniques ou à exercer une respondablité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'nformation tels que définis à l'article 1er de la directive 98/34/CE qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques* ». V. également le CPCE, et son article L32, 15° pour la définition de l' « opérateur ».

[772] De la même manière que le secret des correspondances écrites a d'abord visé les agents des Postes. Le code pénal de 1810 n'incriminait ainsi sa violation que s'agissant de ces fonctionnaires. Il faut attendre une loi de 1922 pour que les particuliers soient également visés. V. : BONFILS P. et E. GALLARDO, « Secret des correspondances », *Rép. Dalloz. Pén..*, actualisation janvier 2016.

[773] V. L'article L33-1 du CPCE. Voir également sur le site de l'ARCEP, la liste des opérateurs déclarés, onglet « opérateurs », www.arcep.fr

encore[774], la possibilité de converser sur le réseau via des logiciels tel *Msn messenger*[775] laissait déjà présager que d'autres applications de communication allaient se développer et venir troubler les définitions traditionnelles d'opérateurs de communication. Si aujourd'hui les règlementations visant ces deux types d'acteurs tendent à s'uniformiser[776], il faut rappeler que c'est la liberté pour un individu d'être mis en relation avec autrui qui doit être protégée et ce par la création d'un secret qui vise en premier lieu l'acte de correspondance et non les données produites et les acteurs qui les collectent.

400. **L'exemple de la différenciation maladroite des « données relatives au trafic » et des « données de localisation »**. Par ailleurs la directive de 2002 définit à la suite des données relatives au trafic les « *données de localisation* ». Ce sont « *toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal de l'utilisateur d'un service de communications électroniques accessible au public* »[777].Or il est difficile de comprendre si de telles données relèvent des données relatives au trafic alors que d'un point de vue technique ces données sont bien émises dans le cadre d'une communication numérique. La suite de la directive ne lève pas l'ambigüité alors que l'article 9 qui organise leur encadrement s'intitule « *Données de localisation autres que les données relatives au trafic* »[778].

La lecture des considérants fait apparaître la logique de cette catégorisation[779]. La donnée relative au trafic localise le point de terminaison du réseau utilisé (antenne relais de la téléphonie mobile, point de terminaison de la boucle locale du réseau filaire, par

[774] *Skype* est un service de VoIP (Voice over IP) qui permet via un logiciel de passer des appels téléphoniques ou vidéos via Internet. Il a été crée en août 2003, v. l'entrée « skype » sur le site wikipédia.org.

[775] Msn Messenger est un service de messagerie instantanée qui permet via un logiciel de discuter (« to chat » en anglais) avec des contacts qui utilisent eux aussi le logiciel. Sa création date de juillet 1999, v. l'entrée « Msn Messenger » sur le site wikipédia.org.

[776] Alors qu'en France l'ARCEP requiert depuis plusieurs années de Skype qu'elle se déclare en tant qu'opérateur pour que la société américaine soit soumise au régime notamment des appels d'urgence et des interceptions de sécurité (V. le communiqué de presse en date du 12 mars 2013 « Skype refuse de se déclarer en tant qu'opérateur », disponible sur le site www.arcep.fr) l'Union européenne réfléchit actuellement à la rédaction d'un code européen des communications électroniques qui visera ces nouveaux services de l'Internet appelés les « OTT » pour « Over-the-top » (tels *Skype* mais également *Whatsapp*, *Hangouts*, *Viber* ou *Wechat*), v. le document de travail émis le 4 octobre 2016, « COMMISSION STAFF WORKING DOCUMENT Executive summary of the evaluation Accompanying the document proposal for a directive of the European Parliament and of the Council establishing the European Electronic Communication Code (Recast) », SWD (2016) 313 final, p.32 disponible sur eur-lex.europa.eu

[777] Directive 2002/58/CE, *op. cit.*, article 2 « Définitions », c).

[778] *Ibid.*, article 9 « Données de localisation autres que les données relatives au trafic ».

[779]La donnée qui révèle « *l'emplacement des équipements terminaux de l'expéditeur ou du destinataire d'une communication* » (Directive 2002/58/CE, cons. n°15 et 35) est bien une donnée relative au trafic qu'il convient d'effacer. La donnée de localisation autre que celle-ci, c'est-à-dire qui ne renseigne pas sur l'établissement d'une communication mais qui renvoie au suivi de la position géographique d'un individu dans le cas de l'utilisation d'un GPS par exemple peut être conservée si elle a été rendue anonyme ou si l'individu a donné son consentement (Directive 2002/58/CE, cons. n°35).

exemple). Les données de localisations renseignent sur la position physique de l'individu via des signaux émis par satellite. La donnée relative au trafic « *qui localise* » vise la position physique du point de départ et du point d'arrivée d'une communication ce qui fait apparaitre un enjeu s'agissant de la liberté d'aller et venir de l'individu puisque celui-ci n'est plus tenu aujourd'hui de se rendre dans un bureau de poste ou de téléphoner de chez lui mais peut se connecter à internet n'importe où. La donnée dite « *de localisation* » renvoie aux différents dispositifs et applications qui proposent d'enregistrer les déplacements d'un utilisateur en vue de la fourniture d'un service. Or la problématique est la même : celle de la géolocalisation d'un individu[780]. Si les régimes qu'il faut imposer à la collecte des ces deux types de données peuvent varier, il faut affirmer un nouveau secret visant le suivi numérique des déplacements physiques d'un individu, ce que malheureusement le droit européen ne fait pas.

b. La logique critiquable de la rétention de telles données.

401. **Le contenu de la directive 2006/24/CE**. La directive 2002//CE dite « vie privée et communications électroniques » prévoit une exception générale au principe d'effacement des données relatives au trafic : elles peuvent être conservées par les États membres dans le but de sauvegarder la sécurité nationale. Une difficulté va apparaître à cet endroit dès lors que les dispositions des États membres en ce sens vont varier considérablement obligeant le législateur européen à établir une nouvelle directive visant l'harmonisation des pratiques.

Au lendemain des attentats de Madrid et de Londres, la directive 2006/24/CE, relative à la conservation des données, est adoptée[781]. Elle est dite en anglais « *directive on retention data »*[782] *;* le terme de « *rétention* » plutôt que celui de « *conservation* »

[780] Le terme de géolocalisation recouvre en effet deux hypothèses : celle de la géolocalisation à son insu d'un individu connecté au réseau, et celle de la géolocalisation d'un individu dans le cadre d'un service dont l'objectif est affiché comme tel. Seule la granularité de la géolocalisation varie qui cible un point du réseau dans l'un et la position réelle de l'individu dans l'autre.

Là encore il est à noter qu'une entreprise comme *Google* avec son moteur de recherche et ses services associés se situe au carrefour de ces deux problématiques ; si l'individu consent à être géolocalisé dans le cadre de l'utilisation d'un service comme *Google Maps,* il apparaît plus ambigu de considérer que son seul consentement permette à Google d'enregistrer sa position géographique à chaque fois qu'il se connecte au moteur de recherche. Une liste de résultats fonction de la position géographique peut résulter efficacement de la seule mention par l'internaute d'un lieu dans la barre de recherche.

Il faut sur ce point souligner que l'activité de Google quand à la localisation d'un individu n'est pas régulée par la directive « vie privée et communication électronique » alors que le service google maps ou celui de moteur de recherche ne relève pas de son champ d'application, de la même manière qu'une entreprise comme Skype n'est pas visée s'agissant des données concernant les appels de ses utilisateurs. L'écueil de la règlementation sectorielle qui vise les opérateurs apparaît à nouveau.

[781] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JOUE 13.4.2006, L105/54-63.

[782] Directive 2006/24/CE « *on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amendin directive 2002/58/CE »*, disponible sur eur-lex.europa.eu. V. également les ouvrages en anglais de Christopher Kuner : KUNER Ch., *European Data Protection Law: Corporate Compliance and Regulation*, 2nd édition, Oxford University Press : 2007, et KUNER Ch., *Transborder data flows and data privacy law*, Oxford University Press : 2013.

apparaît adéquat puisqu'il renvoie davantage à l'acte d'autorité qui conduit à conserver les données qui devraient en principe être effacées une fois la communication achevée. L'article 5 vise six catégories de données à conserver définies selon leurs finalités[783] étant précisé que sont concernés d'une part la téléphonie fixe en réseau et la téléphonie mobile, puis l'accès à internet, le courrier électronique par internet et la téléphonie par internet. Ainsi peuvent être conservées les données permettant d'identifier la source d'une communication, c'est-à-dire le numéro de téléphone attribué ou l'adresse IP attribuée le temps de la connexion, les données permettant d'identifier le destinataire d'une communication qu'il s'agisse d'un numéro appelé ou de l'adresse IP vers laquelle est acheminé un courriel, les données permettant le comptage des appels et des sessions de connexion au réseau internet, les données relatives au mode de communication choisi et les données renseignant sur la localisation physique du point de connexion utilisé.

Il est précisé qu'aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive[784]. L'inviolabilité de la communication est donc sauve mais le secret des correspondances est lui méconnu. La CJUE amenée à se prononcer sur la légalité de la directive au regard des droits garantis au citoyen européen l'invalide dans sa décision du 8 avril 2014.

402. **L'invalidation de cette directive par la CJUE**. De la même manière que la France s'était fait rappeler à l'ordre au début des années 1990 par la CEDH quant à la nécessité de la mise en œuvre d'un régime encadrant les interceptions de sécurité[785], la CJUE va sanctionner le législateur européen en invalidant la directive 2006/24/CE[786]. La problématique ici n'est pas l'absence d'un cadre législatif organisant la surveillance des communications mais l'étendue de celui-ci.

Si l'on peut regretter que la Cour ne fonde pas plus clairement sa décision sur le droit au respect de ses communications reconnu au citoyen européen qui se fond dans la défense de sa vie privée et des ses données personnelles, il faut saluer qu'elle dénonce la

---

[783] V. Directive 2006/24/CE, article 5 « Catégories de données à conserver » : « 1. Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes :

« a) les données nécessaires pour retrouver et identifier la source d'une communication […]

b) les données nécessaires pour identifier la destination d'une communication, […]

c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication, […]

d) les données nécessaires pour déterminer le type de communication, […]

e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel, […]

f) les données nécessaire pour localiser le matériel de communication mobile […] ».

[784] V. Directive 2006/24/CE, article 1, paragraphe 2 et article 5 paragraphe *2.*

[785]CEDH 24 avr. 1990, Huvig et Kruslin c/ France, Série A, n[os] 176-A et 176-B, AFDI 1991. 606, obs. V. Coussirat-Coustère, *D.* 1990. 353, note J. Pradel

[786] CJUE 8 avr. 2014, Digital Rights Ireland c/Ireland C293/12 et C594/12, *D.* 2014, n°23, p.1355 note Castets-Renard, *AJDA* 2014, p.773.

surveillance compulsive que met en œuvre un tel régime de conservation de données. En effet, après avoir reconnu que l'ingérence des autorités nationales dans les droits reconnus par les articles 7 et 8 de la Charte est justifiée par l'objectif d'intérêt général que le régime de conservation vise[787], la Cour questionne la proportionnalité de cette ingérence. Elle est ainsi amenée à considérer les modalités du régime de conservation mis en œuvre et leur adéquation avec cet objectif.

Elle constate à cet endroit le caractère général du régime de conservation des données. Elle dénonce ainsi d'une part que la directive concerne « *de manière globale l'ensemble des personnes faisant l'usage des services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales* » et d'autre part que ladite directive « *ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à un période temporelle et/ou une zone géographique* »[788]. Notant également qu'aucune condition matérielle et procédurale ne vient limiter l'accès de telles données aux autorités nationales compétentes, que la durée de conservation n'est fondée sur aucun critère objectif et que la sécurité des traitements opérés n'est pas suffisamment assurée[789], elle affirme que le principe de proportionnalité n'est pas respecté ce qui conduit à l'invalidation de la directive.

Faisant cela elle met en lumière les travers d'un régime visant en premier lieu des données et non des objectifs fondamentaux.

403. **L'écueil de la « *dataveillance* ».** En effet alors que la logique n'est plus celle d'une mise sur écoute qui nécessite des moyens techniques et financiers, la surveillance ne concerne plus un individu défini eu égard au risque qu'il peut faire peser sur l'ordre public mais organise le traitement des données de l'ensemble des citoyens européens en vue de leur utilisation ultérieure. Il ne s'agit plus de mettre en œuvre la surveillance d'un individu mais de pouvoir accéder à des données lorsqu'une suspicion pèse sur un individu. Apparaît ici le concept de « *dataveillance* ». Les données existent et sont conservées ; elles parleront le cas

[787] *Ibid.*, paragraphes n°38 à 44.

[788] *Ibid.*, paragraphe n°58 et paragraphe n°59. On notera ici la similitude du raisonnement avec les griefs faits par la Cour de Strasbourg en 1990 dans l'arrêt Kruslin alors que le régime des écoutes téléphoniques français ne répondait pas à l'exigence de « prévisibilité de la loi » requis en ne définissant pas notamment les catégories de personnes susceptibles d'être mises sur écoutes ni la nature des infractions pouvant y donner lieu, ni les limites à la durée de l'exécution de la mesure, CEDH 24 avr. 1990, Huvig et Kruslin c/ France, Série A, n^{os} 176-A et 176-B, paragraphe n°35.

[789] *Ibid.*, paragraphes n°60 à 64.

échéant pour établir la culpabilité d'un individu ou informer sur ses contacts et ses déplacements. Or la sauvegarde de l'ordre public et de la sécurité nationale ne peut être invoquée si ne sont pas établies davantage les conditions d'imminence et de proximité du danger qui seules peuvent fonder le traitement.

Il convient d'affirmer que les objectifs visant la protection des libertés individuelles de l'internaute doivent être dissociés et ne peuvent se fondre dans un régime visant les « *données relatives au trafic* ». Comme le premier titre de cette seconde partie l'a montré, il doit être affirmé un principe de fichage des points d'accès qui doivent pouvoir être localisés à partir d'une adresse IP circulant sur le réseau en vue de l'identification de tout internaute connecté au réseau. En revanche le secret des correspondances qui protège la liberté d'expression impose que soient effacées les données visant l'acte de communication en lui-même. Celles-ci ne peuvent être interceptées que s'agissant d'un individu particulier qui a commis une infraction ou présente une menace et suivant une procédure définie.

2) La faiblesse du secret des informations consultées

404. **Les adresses IP des sites visités**. Il a été vu que dès qu'un utilisateur se connecte à internet, une adresse IP lui est attribuée mais toutes les pages du web ont également une adresse IP. Cette adresse obéit toutefois à une logique différente dès lors qu'elle est pérenne dans le temps et que lui a été attribué un nom de domaine. En effet pour faciliter la navigation sur le web, l'adresse IP d'un site web va être associée à un nom de domaine qui est une adresse en langage courant plus facile à retenir que l'adresse numérique[790].

De la même manière qu'un appel téléphonique est dirigé vers le numéro d'un correspondant, la demande de consultation d'un site internet est techniquement dirigée vers l'adresse IP de celui-ci. Au point d'accès au réseau, là où est mise en œuvre la communication, toutes les requêtes auprès des adresses IP des sites web sont visibles et centralisées. Ainsi toute personne attribuant à une connexion une adresse IP valide sur le réseau mondial est à même de considérer le choix de l'internaute parmi les sites du

[790] V. l'avis du G29 34/2000 du 21 nov. 2000 « Le respect de la vie privée sur internet », p.9. C'est l'ICANN (Internet Corporation for Assigned Names and Numbers) qui gère la correspondance entre les adresses IP localisant les sites Web sur le réseau et le nom de domaine qui leur a été attribué selon un système de résolution de nom ou système « DNS » en anglais, qui fonctionne comme un annuaire inversé. Il ne s'agit pas ici d'entrer dans le détail de ce fonctionnement technique mais de considérer que la mise en œuvre de la communication nécessite deux adresses IP. . « La racine du DNS : bien commun ou fragmentation » intervention de Patrick MAIGRON , ingénieur à l'institut Télécom/TélécomSudParis, lors du colloque du CEJEM-Université Panthéon-Assas, « Les philosophie de l'Internet : conciliation possible avec le droit, » du 9 juin 2011.

web en relevant ces adresses IP et en les associant à leurs noms de domaines grâce à un simple outil de type « whois »[791].

De fait le droit européen et français affirme le secret du choix des informations consultées par l'internaute le temps de sa connexion mais d'une manière si peu claire dans le cadre du champ d'application limité des données relatives au trafic que des doutes subsistent sur la conservation de telles adresses IP ou non par les opérateurs.

405. **Le manque de clarté du principe d'effacement des données portant sur les informations consultées**. La directive « *vie privée et communications électroniques* » affirme la confidentialité du contenu des communications qui se prolonge dans celles des informations consultées. Toutefois alors qu'elle organise également un régime d'exception visant la conservation de certaines données relatives au trafic, la frontière s'opacifie entre ces deux régimes ; on ne sait plus quelles données doivent faire l'objet d'un régime dit « d'interception », et quelles données peuvent par exception être « conservées ».

La législation visant les données relatives au trafic semble elle-même faire preuve de pédagogie alors qu'elle martèle que ces données, par exception conservées, ne peuvent viser les informations consultées[792]. De fait ce rappel intervient donc toujours à rebours du régime de conservation et les commentateurs sont perdus ; et ce d'autant que les données sont de même nature –adresses IP attribuées à un point de connexion et adresses IP des sites visités- et détenues par les mêmes acteurs.

Ainsi on peut lire dans un article commentant le décret détaillant les données devant être conservées au titre de l'article L34-1tout juste paru, et qui mentionne que doivent être conservées « *les données permettant d'identifier le ou les destinataires de la communication* » : « *Il s'agit, par exemple, de l'adresse IP du destinataire d'un courrier électronique. Toutefois, il est permis de s'interroger sur la possibilité de conservation des adresses URL des sites visités, ce que le décret ne précise pas* »[793]. De

[791] Whois est la « (*contraction de l'anglais who is?, signifiant « qui est ? ») est un service de recherche fourni par les registres Internet, par exemple les Registres Internet régionaux (RIR) ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine*. », V. entrée « Whois », fr.wikipédia.org

[792] L'article L34-1 énonce ainsi dans son dernier point, le VI, dont la rédaction n'a pas changé depuis 2001 : « *Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices de services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers, sur la localisation des équipements terminaux.*

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ».

En 2006, la directive sur la rétention des données l'affirme à nouveau dans son article 1er « Objet et champ d'application » : « 2. *La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques ».* V. : Directive 2006/24/CE.

[793] LORRAIN A.-C., MATHIAS G., « Données de connexion : la publication du premier décret ou la première pierre d'un édifice encore inachevé », *RLDI,* n °17, juin 2006, p.37.

la même manière sur le site de la CNIL, en 2013, dans un fiche intitulée « Vos traces : les journaux de connexion », il est écrit : « *Les fournisseurs d'accès à internet (FAI) conservent quant à eux un historique des sites auxquels chaque adresse IP sous leur responsabilité a accédé. Par obligation légale, ils les conservent pendant une durée d'un an* »[794]. Une grossière erreur puisqu'au contraire il est prohibé que les opérateurs conservent ces informations de contenus une fois la communication achevée. Leur interception est possible mais relève d'un autre régime qui n'est pas harmonisé puisqu'il ressort de la politique de sécurité publique de chaque État membre.

Ainsi la protection des choix de navigation de l'internaute ne peut ressortir de l'encadrement d'un type de données définies au regard des acteurs qui les collectent, les opérateurs de communications électroniques. La systématisation des données relatives au trafic n'est pas efficace et montre ses limites. L'objet de la protection doit être délimité autrement.

§2) L'ineffectivité du régime visant la mise en œuvre d'un « cookie ».

406. **La définition du « cookie », un témoin de connexion.** Le cookie est un fichier texte déposé par le site web sur le terminal de l'internaute qui se connecte à son service et qui sera recherché par le site lors de toute connexion ultérieure de la même machine[795]. C'est donc l'identifiant sous forme de numéro unique d'une machine pour le site du web qui le met en œuvre[796]. Ainsi il faut différencier ce procédé de l'adresse IP qui est une donnée produite automatiquement par toute connexion au réseau. Le cookie en revanche est un procédé librement mis en œuvre par les sites du web ; le cookie n'est pas nécessaire à la connexion au réseau, il témoigne de la connexion à un site du web.

En effet, la répartition dynamique des adresses IP fait qu'un site web qui voit se connecter à lui, plusieurs fois, la même adresse IP ne peut en déduire qu'elle appartient au même utilisateur. En revanche s'il introduit un fichier texte unique dans le terminal connecté, il sera capable de réactiver celui-ci à chaque nouvelle connexion de la machine et de considérer les reconnexions d'un même terminal. Cette individualisation de chaque machine utilisatrice du service optimise la navigation en ce sens qu'elle

[794] V. sur le site Cnil.fr, dans son architecture au 4 juillet 2007 : rubrique «vos droits », puis « vos traces », puis « les journaux de connexion », «en savoir plus ».

[795] Voir l'entrée « Cookie (informatique » sur le site wikipédia.org.

[796] « Le cookie est un petit fichier texte déposé sur votre disque dur par le serveur du site que vous visitez. Il contient quelques données, notamment, le nom du serveur qui l'a écrit, éventuellement une date d'expiration et le plus souvent un identifiant sous forme d'un numéro unique », v. la définition du « cookie » sur le site de la CNIL, cnil.fr.

permet aux sites de considérer des schémas de connexions et de personnaliser dès lors leurs services.

407. **La fonction d'un « cookie », la personnalisation des services du web**. Une entreprise du web peut collecter différentes données s'agissant des connexions à ses sites et services. Ces données sont enregistrées dans ce que l'on appelle des « fichiers-journaux » ou « log-files » en anglais[797]. Ces fichiers peuvent à l'origine être mis en œuvre librement par les sites du web alors qu'ils sont constitués de ce que l'on appelle à bon escient des « *données de bavardage* » : en ce sens qu'elles ne révèlent rien sur la personne connectée et ne sont donc pas intrusives s'agissant de sa vie privée.

Le groupe de l'article 29 précise ainsi qu'elles comprennent d'habitude les informations suivantes : « *-le système d'exploitation de l'utilisateur Internet, -type et version de son navigateur, protocoles employés pour surfer, page qui a transféré le visiteur vers le site, préférences linguistiques, - cookies* »[798]. Ainsi par exemple un site web peut considérer à partir de celles-ci l'étendue du trafic des connexions en provenance d'un site web spécifié, la nationalité des connexions à son site, et la popularité des pages de son service qui peuvent être classées selon le nombre de visites.

La mise en œuvre d'un cookie va alors permettre un ordonnancement de ces fichiers journaux au regard d'un numéro unique désignant une machine. En effet sous ce numéro unique différentes informations relatives à l'utilisation du service peuvent être stockées. Ainsi comme l'explique le Forum des droits de l'Internet dans sa recommandation sur la « Publicité ciblée sur Internet » en date du 8 mars 2010, il existe différents types de cookies : peuvent être cités notamment « *les « cookies de session » qui permettent le stockage d'informations liées à la session de navigation de l'internaute (paramètres de connexion à un service, contenu du panier d'achat, etc.), les « cookies de personnalisation » qui permettent de conserver des informations sur l'utilisateur et de les réutiliser lors de ses prochaines visites (préférence d'affichage, information de connexion à un service, etc.) et « les cookies de tracking ou cookies traceurs » qui permettent de connaître l'historique de navigation d'un utilisateur (liste des pages visitées, identifiées par leur URL, et ordre de visite)* »[799]. Il est précisé qu'un même cookie peut être à la fois de session, de personnalisation ou traceur.

[797] Le terme « log » renvoie aux journaux de bord des marins tenus à l'origine sur des rondins de bois.

[798] Avis du G29, WP 37, du 21 novembre 2000, sur « Le respect de la vie privée sur Internet- une approche européenne intégrée sur la protection des données en ligne », p. 46/47.

[799] V. la recommandation du Forum des droits sur l'internet sur la « Publicité ciblée sur Internet » en date du 8 mars 2010, p.9.

408. **La problématique de la protection des données personnelles de l'internaute**. Il apparaît alors que cette collecte de données au regard d'une même machine utilisatrice du service peut révéler des informations sur l'utilisateur notamment eu égard aux cookies traceurs ou dits « *de navigation* ». Cette collecte de données opérée par les services du web grâce aux cookies questionne dès lors le respect de la vie privée de l'internaute connecté au réseau et la protection de ses données personnelles puisqu'un numéro unique centralise ses préférences de connexions et ses choix de navigation sur un site web.

Toutefois là encore les débats sont vifs ; ils portent de la même manière que pour l'adresse IP sur les critères permettant de considérer si le site web a affaire à un individu identifiable ou non. Pour certains l'identité de l'internaute, quand bien même ses préférences ou ses choix de navigation sont conservés, n'est pas connue du site web ; pour d'autres cette collecte de données présente un risque alors qu'elle peut permettre de découvrir l'identité de l'internaute, qui peut par ailleurs s'être authentifié et prétendre à ce que sa navigation ne soit pas connue.

Or il faut à cet endroit considérer à nouveau qu'il faille s'extraire de la logique de la mise en œuvre d'un fichier de données personnelles. Il faut envisager qu'un site web est fondé à considérer les choix de connexions à son service qui limités quant à leur étendue ne permettent pas une identification automatique de l'internaute connecté derrière le terminal individualisé par le numéro du cookie. Par ailleurs quand bien même l'utilisateur s'est authentifié et qu'alors le site web collecte des informations au nom de celui-ci, la logique reste celle de la personnalisation des services nécessaire au fonctionnement du web. La problématique n'est pas celle du suivi de la navigation d'un internaute et d'une possible identification à partir des données collectées mais celle de l'exploitation des données collectées en vue de son profilage. Il ne s'agit pas d'envisager alors une atteinte à la vie privée de l'internaute mais de considérer le risque de l'uniformisation des contenus voire de l'orientation des choix de l'internaute grâce au datamining et à la puissance des algorithmes.

409. ***Plan.*** Ainsi l'étude du contenu de la législation visant la mise en œuvre d'un cookie **(A)** conduit à considérer qu'il faille affirmer la liberté pour les sites web de mettre en œuvre un tel procédé **(B).**

A] Le contenu du régime visant la mise en œuvre d'un cookie

410. ***Plan.*** La législation visant à encadrer la mise en œuvre des cookies a beaucoup évolué ces dernières années **(1)** Elle oblige aujourd'hui au recueil du consentement de l'internaute, une prescription qui montre ses limites **(2).**

1) L'évolution du régime de la mise en œuvre d'un cookie

411. **Le développement des cookies à la fin des années 1990**. Le cookie est un procédé inhérent à l'application web alors que la mise en œuvre de schémas de connexions permet une navigation effective et optimisée. Dès la fin des années 90, ces fichiers textes sont mis en œuvre par les sites du web qui ne consistent à l'époque qu'en des pages de contenus que l'internaute souhaite consulter alors que le web participatif commence tout juste à émerger et qu'il ne s'agit pas encore de se loguer pour accéder à un service dans le cadre du web applicatif.

Alors que beaucoup d'incertitudes pèsent sur ces procédés parfois appelés « mouchards »[800], les éditeurs de sites qui font appel à eux informent les internautes de leur mise en œuvre et requièrent leur consentement. En effet le dépôt dans leur ordinateur d'un tel fichier peut s'apparenter notamment à une intrusion frauduleuse dans un système informatique, intrusion sanctionnée pénalement en droit français[801].

Ainsi à l'orée des années 2000, de plus en plus de fenêtres « pop-up »[802] apparaissent dès que l'on navigue vers un site sur lesquelles il convient de cliquer pour pouvoir accéder au contenu. De fait il est noté que le consentement est forcé puisque si le cookie n'est pas accepté, il est souvent difficile d'accéder au site[803]. L'internaute en vient à cliquer machinalement sur ce message d'avertissement[804] ; le « surf » sur le web pour utiliser une expression emblématique de l'époque en est passablement ralenti.

Il apparaît alors que le consentement de l'internaute à un tel procédé ne peut être requis et en Europe la directive 2002/58/CE va alors consacrer la liberté de mise en œuvre d'un cookie sous réserve que l'internaute soit en mesure de s'y opposer.

412. **La directive 2002/58/CE « vie privée et communications électroniques » : le régime de « l'OPT-OUT »**. La directive 2002/58/CE dite « vie privée et communications

800 LUCAS André, DEVEZE Jean, FRAYSSINET Jean, Droit de l'informatique et de l'Internet, Paris : P.U.F., 2001 (Thémis Droit privé), p. 15-16.

[801] V. le délit introduit par la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique et dite loi « Godfrain ». Ce délit est actuellement prévu à l'article 321-3 du code pénal.

[802] « *Un ou une pop-up (de l'anglais pop-up window ou pop-up tout court), parfois appelée fenêtre intruse ou fenêtre surgissante, est une fenêtre secondaire qui s'affiche, sans avoir été sollicitée par l'utilisateur (fenêtre intruse), devant la fenêtre de navigation principale lorsqu'on navigue sur Internet.* », v. l'entrée « Pop-up» sur le site wikipédia.org.

[803] LUCAS André, DEVEZE Jean, FRAYSSINET Jean, *Droit de l'informatique et de l'Internet*, Paris : P.U.F., 2001 (Thémis Droit privé), p. 15-16.

[804] Un message par ailleurs souvent rédigé en anglais.

électroniques » opère d'abord une précision utile en distinguant les logiciels malveillants qui cherchent à suivre les activités d'un internaute, des « *témoins de connexion (cookies)* » qui « *peuvent constituer un outil légitime et utile »*[805].

S'agissant dès lors de ces témoins de connexion, un régime dit « d'OPT-OUT » est décidé : le cookie est mis en œuvre sans le consentement de l'internaute mais ce dernier informé de la mise en œuvre de celui-ci doit être à même de pouvoir s'opposer à une telle implantation[806]. Il est ainsi fait mention dans la législation communautaire d'un *« droit de refus* » dont les contours apparaissent toutefois peu clairs. En effet ce droit de refus implique donc de proposer à l'internaute un moyen de refuser tout cookie ce qui renvoie à une sollicitation à chaque implantation de fichier tout comme au temps où le consentement était demandé par les sites. La directive précise que les méthodes retenues doivent être « les *plus conviviales possibles* »[807] et indique par ailleurs que « *L'accès au contenu, d'un site spécifique peut être, toutefois, subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion »*[808]. Il est ainsi possible que des sites ne mettent pas en œuvre le droit d'opposition.

En France, l'article 32-II de la loi Informatique et Libertés prévoit que tout internaute soit informé par le responsable du traitement réalisé par le cookie de la finalité de celui-ci et des moyens dont il dispose pour s'y opposer[809]. Ainsi en réalité le régime de « l'OPT-OUT » impose qu'un internaute soit informé des cookies déposés dans sa machine et qu'il puisse a posteriori supprimer ceux-ci s'il le souhaite. Dès lors les fenêtres « pop-up » ont disparu et ont été mis en œuvre des pages et formulaires spécifiques permettant à l'internaute de considérer les cookies déposés dans sa machine et de les paramétrer selon ses propres choix a posteriori de leur implantation. Cependant cette logique a montré ses limites alors que l'information de l'internaute était moins efficace et que de fait une telle gestion des cookies était trop complexe pour lui. Il a alors été décidé lors de la révision du Paquet Télécom en 2009 de réintroduire l'exigence de consentement.

---

[805] [805] Dir. 2002/58/CE concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques, v. cons.24 et 25, JOCE 31.7.2002, L201/37-43

[806] *Ibid.*, article 5, 3.

[807] *Ibid.*, cons. 25.

[808] *Ibid*.

[809] L'article L32 II. est ainsi rédigé : « Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant : - de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ; - des moyens dont elle dispose pour s'y opposer […] ».

413. **La révision du Paquet Télécom en 2009 : le régime de « l'OPT-IN ».** En 2009 alors qu'il est considéré qu'il est « *extrêmement important* » que les utilisateurs soient informés de tout stockage de fichiers sur leur machine et des accès aux informations qu'ils contiennent, il est décidé de revenir à un régime d' « OPT-IN » qui seul permet cette information[810]. Ainsi le cookie ne peut plus être implanté par défaut, il faut que l'internaute consente à sa mise en œuvre.

L'article 5 paragraphe 3 de la directive 2002/58/CE est réécrit. Il est ajouté en 2011[811] un alinéa à l'article 32.II de la loi Informatique et Libertés française qui énonce désormais que : « *Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle* ».

Dès lors les sites web se mettent en conformité avec la nouvelle législation et comme au début des années 2000, des bannières fleurissent sur le web. Or la généralisation de tels procédés questionne de la même manière qu'à l'époque le sens du recueil du consentement de l'internaute alors que celui-ci est amené à cliquer machinalement sur celles-ci pour poursuivre sa navigation.

2) L'ineffectivité de l'obligation de consentement à la charge de l'internaute

414. **Les paramètres actuels de recueil de consentement de l'internaute**. Pour opérer l'information requise par l'article 32. II de la loi Informatique et Libertés et recueillir le consentement de l'internaute, les sites web mettent en œuvre à l'origine des bannières qui détaillent les finalités poursuivies par les cookies mis en œuvre[812] et demandent à l'internaute de cliquer sur « *ok* » ou « *j'accepte* » pour obtenir son consentement ; un lien actif permettant également d'obtenir plus d'informations sur la politique de confidentialité du site ou sur celle visant la gestion de ses cookies. La CNIL souligne en effet que la validité du consentement est liée à la qualité de l'information reçue mais précise toutefois que « *l'utilisation d'une*

[810] V. : cons. 66, directive 2009/136/CE du 25 novembre 2009 du Parlement européen et du Conseil modifiant la directive SERVICE UNIVERSEL et la directive VIE PRIVEE ET COMMUNICATION., JOUE 18.12.2009 L337/11.

[811] Ordonnance n°2011-1012 du 24 Août 2011 relative au communications électroniques, JORF 26 Août 2011, texte 49 sur 134, article 37.

[812] Ainsi les formules s'agissant des finalités varient : «notamment à des fins promotionnelles et/ou publicitaires dans le respect de notre politique de protection de la vie privée » (application M6 replay), « afin de vous assurer la meilleure expérience possible sur notre site Web » (site de vente en ligne shopstyle.fr), « les cookies assurent le bon fonctionnement de nos services » (messagerie *Gmail* de *Google*), « vous acceptez l'utilisation des cookies relatifs à la publicité, aux réseaux sociaux et à la mesure d'audience » (site de l'INA.fr), « vous acceptez l'utilisation de cookies pour vous proposer des publicités adaptées à vos centre d'intérêts, réaliser des statistiques, ainsi qu'interagir avec des réseaux sociaux » (site Larousse.fr), « vous acceptez l'utilisation de cookies qui permettront notamment de vous offrir, contenus, services, et publicités liés à vos centres d'intérêts » (site commentcamarche.net du groupe Benchmark).

terminologie juridique ou technique trop complexe ne répondrait pas à l'exigence d'une information préalable » [813].

Toutefois ce procédé évolue et les bannières toujours aussi nombreuses puisque légalement requises se contentent souvent aujourd'hui d'indiquer : « *En poursuivant votre navigation sur notre site, vous acceptez que nous utilisions des cookies conformément à notre politique de protection de votre privée »*. Le clic, le plus souvent sur une croix, permet alors de fermer la bannière qui de fait n'empêche pas la navigation et ne masque pas le contenu du site. Toutefois agissant comme une pollution visuelle et un frein à la navigation, l'internaute clique pour fermer le message et ne plus le voir apparaître à sa prochaine connexion au même site.

415. **L'absence de réel consentement de l'internaute**. Dès 2009, alors que le régime de « l'OPT-IN » est adopté, les conséquences pratiques de sa mise en œuvre sont dénoncées. Les praticiens concluent alors à une interprétation pragmatique de la réforme ne pouvant envisager un retour en arrière et une multiplication des fenêtres « pop-up »[814]. L'atteinte à la fluidité de la navigation est rappelée : « *Si l'internaute choisit d'autoriser individuellement chaque cookie au cas par cas, il se retrouve avec un nombre incessant de messages de confirmation qui deviennent vite pénalisants pour la navigation »*[815]. Mais dans les faits la mise en œuvre des prescriptions légales visant expressément désormais l'accord de l'intéressé va donc conduire à ce clic supplémentaire nécessaire pour accéder à tout site du web.

Aujourd'hui ce régime légal est dénoncé, notamment par la presse étrangère, qui prend du recul face à cette pratique européenne. Le *New York Times* écrit ainsi que l'exigence de consentement s'agissant des « cookies » s'est transformée de manière générale en une gêne agaçante sans pour autant que les entreprises du web aient opéré des changements significatifs dans leurs pratiques[816]. En effet si cette politique a pu mettre l'accent à l'origine sur les pratiques des sites web et sensibiliser les internautes à celles-ci, il faut affirmer qu'il n'est pas de la responsabilité de l'internaute de gérer des

[813] V. : Article 2, CNIL, Délibération n°2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978, JORF n°0299 du 26 décembre 2013, Texte n°101.

[814] CORDIER G., « Focus sur la directive 2009/136/CE du 25 novembre 2009 modifiant la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques : optons pour une interprétation pragmatique des cookies », *RLDI*, n°57, février 2010, p. 1904.

[815] CNIL, *La publicité ciblée en ligne*, communication présentée en séance plénière le 5 février 2009, par B. Peyrat, rapporteur, p. 24. (disponible sur le site cnil.fr).

[816] "Another 2011 European law requiring websites to alert visitors to "cookie" trackers that collect data on browsing history has largely turned into a distracting annoyance rather than changing how companies operate. People often accept the tracking to get rid of the pop-up warning without reading details about the tracking.", D. WAKABAYASHI, A. SATARIANO, « How Facebook and Google could benefit from the G.D.P.R, Europe's New Privacy Law », article mis en ligne sur le site du New York Times, le 23 avril 2018.

cookies et que de manière pragmatique, il n'est tout simplement pas capable de le faire en considération de ses connaissances techniques. Le consentement ne peut être éclairé et n'est jamais effectif alors que l'individu ne peut considérer par lui-même les tenants et aboutissants de sa protection eu égard à la collecte de données que les sites du web peuvent mettre en œuvre.

Il faut organiser le respect de l'anonymat de l'internaute connecté au réseau qui n'est pas mis en danger par la collecte de données de navigation via un cookie tant que celle-ci est fragmentée. La logique doit être celle de la liberté pour les entreprises du web de mettre en œuvre un tel procédé. Une réflexion doit être menée autour du profilage permis qui doit être encadré mais qui en soi ne menace pas les libertés individuelles de l'internaute.

B] La liberté pour les sites et services du web d'implanter un cookie

416. **Le périmètre de la navigation concernée.** Alors que l'espace métrique ne se retrouve pas sur le réseau, il peut être difficile de considérer dans quelle mesure doit être interdit le suivi d'un internaute. Toutefois une analogie apparaît si l'on considère le web comme un espace et les sites et services disponibles comme des magasins ou des immeubles le constituant.

Il faut dès lors différencier le suivi d'un individu naviguant parmi les pages d'un site web et le suivi d'un individu naviguant parmi les sites et services de la Toile. Les problématiques ne sont pas les mêmes. Le premier suivi peut s'envisager sous l'angle de la liberté d'entreprendre du site web qui doit être libre de considérer la navigation sur ses pages de ses utilisateurs alors que cela participe du fonctionnement même d'un service dématérialisé qui doit pouvoir interagir avec ses utilisateurs. Il est une problématique à cet endroit s'agissant du profilage de l'internaute mais celle-ci ne porte pas atteinte à la liberté d'accès et de navigation de l'internaute **(1).** A l'inverse celles-ci sont méconnues dès lors qu'est visualisé l'ensemble des choix de l'internaute connecté ce qui permet une identification à son insu **(2).**

1) La nécessaire interaction avec l'utilisateur du service

417. **La nécessaire interaction avec l'internaute utilisateur du service**. En mettant fin à la fiction qui est celle d'un consentement au dépôt d'un cookie, la problématique du traçage qui peut s'opérer sur le web apparaît plus clairement.

Les entreprises du web sont fondées à considérer les pérégrinations d'un internaute parmi les pages de leurs services alors que ce suivi réalise la nécessaire interaction qu'il doit y avoir avec l'internaute connecté. Comme le souligne El Hassan Bezzazi, maître de conférence en informatique à l'Université de Lille 2, dans un article intitulé « Identité numérique et anonymat : concepts et mise en œuvre » : « *Dans un contexte commercial, le profilage est la première fonction consommatrice de ces données et n'a pas a priori besoin de l'identité mais seulement de la personnalité* »[817]. Cette assertion fait référence à la logique du marketing[818] qui vise à adapter l'offre à la demande mais n'a pas besoin pour cela de connaître les coordonnées des clients.

Ainsi la collecte de données par les entreprises du web s'inscrit dans l'évolution tout à la fois de la vente à distance qui a toujours été marquée par la collecte de l'historique des commandes et la volonté d'une personnalisation des offres mais également de celle de la diffusion des contenus qui nécessairement doit considérer un ciblage de ses audiences. Or sur le réseau, dématérialisé, il faut considérer que puissent être enregistrés non seulement les historiques de commandes mais également la navigation parmi les offres proposées et les pages et informations mises en ligne.

En effet ce relevé permet la nécessaire interaction qu'il doit y avoir entre un internaute et le service qu'il utilise. En matérialisant les centres d'intérêts de l'internaute, il permet de délivrer des suggestions d'achats personnalisées de la même manière qu'un vendeur interrogeant un client dans le monde physique le conseille ou qu'à la télévision les publicités sont fonction du programme et de l'audience visée. Ce suivi trouve son fondement dans la dématérialisation même des services et de leurs contenus : ils doivent être proposés de manière proactive à l'internaute qui ne peut appréhender concrètement leur étendue. Le procédé du « cookie » est inhérent au web ; il participe de sa fonctionnalité et de son économie.

418. **L'enjeu de l'uniformisation des offres et contenus**. Par ailleurs l'internaute peut mettre en œuvre techniquement des mécanismes pour ne pas être suivi, comme celui appelé « Do Not Track »[819]. Il faut souligner qu'actuellement ces procédés n'interviennent qu'à la

[817] BEZZAZI El Hassan, « Identité numérique et anonymat : concepts et mise en œuvre », in «La sécurité de l'individu numérisé, réflexions prospectives et internationales », Paris : L'Harmattan 2008, Stéphanie LACOUR (*dir.*), p.77.

[818] Le marketing est « l'ensemble des actions permettant d'adapter la demande à l'offre. […] La démarche marketing consiste à mettre l'offre en avant afin de susciter une demande. […] De manière générale, les innovations radicales sortent rarement de l'imagination des consommateurs ». V. SOULEZ S. *Le Marketing*, Paris : Gualino Extenso editions : 2008 (coll. Les Zoom's), p. 21-22. Dans cet ouvrage l'auteur explique comment l'on est passé d'un marketing de masse à un marketing « one-to-one », un marketing qui va plus loin que le marketing relationnel en ce sens qu'il individualise vraiment la relation avec le client (individualisation de la relation, connaissance du client, écoute du client, production à la demande et mémoire du client).

[819] Le « Do not track » est techniquement un en-tête http envoyé par le navigateur au site Web qui lui permet de considérer que la connexion opérée ne souhaite pas qu'on la suive. D'une manière plus générale, cette expression désigne

marge ; généralisés ils mettraient selon certains en péril la fonctionnalité et l'économie du web. Alors que ces procédés se démocratisent, leur peu de prégnance ne peut plus être mise sur le compte de l'insuffisance des connaissances techniques des internautes.

D'autre part il faut relever que la mise en œuvre d'une publicité ciblée ou d'une mesure d'audience ne porte pas atteinte en soi à l'individu. Le suivi des clics d'un internaute sur un site web ne porte pas atteinte à sa liberté individuelle. De deux choses l'une : soit celui-ci s'opère anonymement ce qui n'a pas de conséquence pour l'individu, soit il renvoie à un individu identifié dans le cadre de la création d'un compte client. L'enjeu du consentement intervient à ce niveau : l'internaute ne peut être contraint de s'identifier pour naviguer ou consulter des offres et des informations. La problématique est ici avant tout celle de l'uniformisation des offres et peut-être même de leur appauvrissement d'un point de vue culturel[820] ; une problématique qui, plus largement, renvoie à l'encadrement de l'intelligence artificielle qui exploite les bases de données mises en œuvre et organise l'architecture des services en conséquence.

En réalité ce qu'il convient d'interdire est un suivi qui par ses caractéristiques même menacerait la libre détermination de l'individu.

---

l'initiative qui consiste à vouloir standardiser cette solution de protection contre le traçage publicitaire. La principale difficulté du système est qu'il repose sur une collaboration avec les sites Web et l'accord des sociétés de tracking. V. : l'entrée « Do no track » sur le site wikipédia.org. HINAULT R., "Le W3C crée un groupe de travail pour la protection anti-traçage/ Google et Opéra continue de tourner le dos à Do not Track », article mis en ligne le 12 septembre 2011 sur le site developpez.com, « Anti-tracking : Mozilla dévoile sa solution pour Firefox », article mis en ligne le 24 janvier 2011 par jérôme G. sur le site generation-nt.com.

[820] Sur l'enjeu des algorithmes qui hiérarchisent la visibilité de l'information, v. les travaux du sociologue Dominique Cardon. CARDON D., « L'identité comme stratégie relationnelle », *Hermès La Revue*, n°53, 2009, p. 61 et également son allocution lors du colloque organisé par le M2 Droit du multimédia et de l'Informatique de l'Université de Paris 2, « Les réseaux sociaux, quels enjeux juridiques », le 6 mars 2009.

D'une manière plus générale l'historien François Bedarida dans un article intitulé « Histoire et pouvoir dans 1984 » parle d'âge d'uniformité *« De 1948 à 1984 –deux dates aux chiffres simplement inversés- une trentaine d'années ont suffi pour que l'humanité en arrive à l'âge de l'aliénation totale de l'individu : l'âge de l'uniformité, l'âge de la solitude, l'âge de Big Brother. Anti-utopie, ou, selon l'expression de Anthony Burgess dans 1985, « catatopie », le livre préfigure un avenir terrifiant contre lequel il sonne l'alarme […] Le conformisme universalisé, aseptisé, intériorisé ?* » V. BEDARIDA François « Histoire et pouvoir dans 1984 » in Vingtième siècle, revue d'histoire, n°1 janvier 1984, p.8. Le professeur de droit canadien David. H. Flaherty énonce pour sa part que le « *storage of personal data can be used to limit opportunity and to encourage conformity* », v. -FLAHERTY D. H. « Protecting privacy in surveillance societies, The Federal Republic of Germany, Sweden, France, Canada, and the United States" UNC Press Books, 1 févr. 1992.Enfin Mireille Delmas-Marty souligne cette problématique en ces termes : « *En rendant accessible le vieux rêve d'une bibliothèque universelle, la numérisation, comme toute technique nouvelle s'avère donc ambivalente. Elle suscite à la fois un « bonheur extravagant » (Borges) à l'idée d'avoir accès à tout le savoir de l'humanité, dans sa diversité même, et des paniques, quand on songe, bien au-delà des droits d'auteur, aux supports détruits, comme il l'ont commencé à l'être à partir de l'usage des microfilms, et surtout au risque d'éradiquer toute diversité en uniformisant les cultures* » DELMAS-MARTY Mireille « La refondation des pouvoirs » in *Les forces imaginantes du droit (III)*, Paris : Seuil 2007 (coll. La couleur des idées), p. 249.

Ces propos font écho aux pratiques des nouveaux services de contenus en ligne dont la plus-value est non seulement l'étendue de leur offre mais également leur système de recommandation. Par exemple le service du géant américain Netflix qui repose sur un algorithme pour proposer des contenus pertinents fonction de l'utilisateur. Ainsi « *Huit cent personnes travaillent sur le « big data » » chez Netflix, dont un tiers d'ingénieurs. Neil Hunt* –responsable produit chez Netflix- *révèle que son équipe fait énormément de tests. « Nous expérimentons sur un demi-million d'utilisateurs [à leur insu] et nous regardons ce qui fonctionne le mieux », précise-t-il. Neil Hunt s'est par exemple rendu compte qu'en choisissant une image plutôt qu'une autre pour « Breaking Bad », le nombre de visionnages n'était pas le même. »*, V. GRONDIN A., « Netflix mise sur la recommandation », *20minutes*, mardi 16 septembre 2014, p.15.

2) *La prohibition de considérer l'ensemble des choix de connexion d'un internaute*

419. **L'ensemble des choix de connexion de l'internaute**. La navigation qui doit faire l'objet du secret est celle opérée sur le réseau et non celle parmi les pages d'un site qui ne révèlent que des centres d'intérêt de la personne et non ses faits et gestes La pratique de mesure d'audience des pages visitées ne peut se comprendre que parce que le site web n'a connaissance que d'une partie de la navigation de l'internaute, celle qui concerne ses propres services. Alors que la navigation suivie n'est que parcellaire, elle ne permet pas d'identifier l'individu derrière son ordinateur.

A cet endroit il convient d'être vigilant sur la centralisation des services du web applicatif et la mise en œuvre de diverses régies publicitaires. Il ne faudrait pas qu'en multipliant les services associés ou en couplant les données de divers sites via une régie, le gisement de données soit tel qu'il permette une identification de l'internaute à son insu, identification qui irait à l'encontre du principe d'anonymat sur le réseau**.** Toutefois il faut constater que même à travers la mise en œuvre de régies publicitaires ou à travers, par exemple, le développement du bouton « J'aime » de Facebook sur diverses pages et services du web[821], la collecte de données est nécessairement contextualisée. Elle est relative à des achats ou à des centres d'intérêts mais ne révèle pas l'ensemble des sites qui ont été visités par un internaute sur le web le temps de sa connexion[822].

Disant cela il apparaît que le périmètre des données visées n'est pas fonction de leur définition technique, ni même des acteurs qui les collectent, il s'attache à considérer à quels niveaux s'opère une collecte de données qui réalise une centralisation des choix de navigation d'un internaute sur l'ensemble des sites du web qui permettent de suivre l'internaute le temps de la connexion et de l'identifier à son insu.

Section II. Le régime du secret de la navigation de l'internaute

420. **Le régime d'une liberté publique.** Le mouvement de développement des droits de la personnalité a mis l'accent ces dernières années sur le respect de la vie privée et a conduit à

[821] V. GIRARD L., « L'exploitation des informations privées à des fins commerciales aiguise les appétits », *Le Monde,* du vendredi 28 mai 2010, p.17.

[822] Comme le souligne le professeur de droit américain, Daniel J. Solove dans son ouvrage *The digital person* : «*Altough the digital biography contains a host of details about a person, it captures a distorted persona, one who is constructed by a vartiey of external details. Altough the information marketers glean about us can be quite revealing, it still cannot penetrate into our toughts and often only partially captures who we are",* SOLOVE D., *The digital person, technology and privacy in the information age*, New-York University Press, 2004, p.45

réfléchir aux limites d'un droit à l'autodétermination de l'individu s'agissant des informations qui le concerne. Cette réflexion est venue empiéter sur celle visant l'encadrement de la surveillance et le respect de la personne physique[823]. Le concept de vie privée initialement lié à la défense de la personne « *dans son existence même* »[824] a été élargi pour faire de la volonté de l'individu l'objet de la protection. Faisant cela paradoxalement le lien a été rompu avec l'objectif de protection de la liberté individuelle.

La subjectivisation déplace le point d'équilibre. D'une part la protection en visant non plus la personne physique mais les informations qui la concernent s'est affaiblie car le secret de la vie privée ne peut plus alors avoir valeur de principe. D'autre part, le rôle de l'État se dilue dans l'affirmation « d'un droit à », alors que cette exigence rend l'enjeu de pouvoir s'agissant de l'intrusion dans la vie privée moins visible. Ainsi le phénomène de dilution du droit au respect de la vie privée dans un droit à la protection pour l'individu de ses données personnelles qui vise la protection d'un objet, des données, avant que de définir des objectifs à atteindre, stoppe tout effort de définition d'obligations légales générales[825] ayant valeur de principes. Il convient ici en effet de considérer que la matrice d'un droit subjectif tel le droit à la vie privée ne peut être effective dès lors que la matérialisation de la navigation d'un internaute, via la production de données techniques, ne relève pas d'une intrusion volontaire dans un espace que l'individu souhaite protéger mais se réalise automatiquement et à son insu.

Ainsi s'il peut apparaître en creux la consécration d'un droit pour l'individu à une navigation anonyme sur le web dès lors que l'internaute peut arguer que personne n'a à connaître de ses allers et venues parmi les sites et services du web, le choix est fait ici de ne pas adopter une formulation subjective qui ne fait pas apparaître clairement les limites du régime à mettre en œuvre. La logique doit être ici celle de la protection d'une liberté publique.

---

[823] Comme le souligne Paul Shiff Berman, professeur de droit à la George Washington University : "*Indeed the entire idea of "informational privacy" has in some respects replaced traditional privacy concerns about surveillance as the principal subject of debate*". BERMAN P. S., *Law and society approaches to cyberspace.* 2007, Ashgate Publishing (The international library of essays in law and society), introduction p. XVIII. V. également l'article de Julie COHEN, professeur au Georgetown University law Center : COHEN J. « Examined lives : informational privacy and the subject as object", *Stanford Law Reviexw*, n°52, may 2000, 1373.

[824] L'on rappellera que le secret de la vie privée a émergé avec l'essor des moyens de captation modernes ; il renvoyait alors directement au lieu physique où la personne se trouvait et condamnait une intrusion d'autrui dans la « sphère privée ». Il est indissociable également du développement de la presse dite « à scandale ».

L'expression est empruntée ici au Doyen Decocq qui affirme : « *Enfin, si l'on médite sur le fondement de la protection du secret du vivant, prolongement de celle de la liberté physique, on est contraint d'admettre que l'inadmissible est qu'une personne puisse être observée contre son gré, dans son existence même.* ». V. DECOCQ A., « Rapport sur le secret de la vie privée en droit français », *in Le secret et le droit*, Travaux de l'Association Capitant, tome XXV, 1974, p.479

[825] Nous empruntons cette expression à Herbert Maisl. V. : HUET Pierre (*dir.*), *Le droit du multimédia, de la télématique à Internet*, Paris : Les éditions du téléphone, 1996. (Rapport de l'AFTEL : association française de la télématique et du multimédia), contribution de Herbert Maisl « La protection des données et des systèmes », p. 167.

421. **Le choix du mot « secret ».** Le terme « secret » est emblématique de la fin des années 70 et des années 80 : sont garantis le « *secret des correspondances* »[826], le « *secret des choix faits par les personnes parmi les services de télécommunication et parmi les programmes* »[827]. Sont étudiés le « *secret des fichiers* »[828] et le « *secret de la vie privée* »[829]. Puis le « secret » est remplacé par le terme de « confidentialité » notamment dans les textes communautaires[830]. Les deux termes sont alors employés indifféremment[831].

Toutefois il faut différencier le mot « secret » de la « confidentialité » héritée de la « *confidentiality* » anglo-saxonne qui renvoie davantage au monde des affaires, en ce qu'elle désigne non pas un domaine protégé mais un ensemble de règles encadrant la divulgation de l'information[832]. Ce terme est associé au « *breach of confidence* » que l'on traduit difficilement en français et qui renvoie également à une relation contractuelle : il y a rupture de la confidentialité promise[833]. Ainsi le mot « confidentialité » met l'accent sur le risque de « révélation » qui s'envisage naturellement alors qu'il est encadré par une série de règles dans le cadre d'une relation bipartite[834].

La portée du mot « secret » est autre : il met l'accent sur l'individu et son intimité. Il renvoie à la garantie d'un domaine réservé avant d'en organiser la divulgation. Si un document confidentiel est déclassifié selon un anglicisme qui renvoie là encore au caractère anglo-saxon de la confidentialité, un secret se garde. Le secret est de droit public et doit être garanti.

422. ***Plan.*** Dans un premier temps, il sera vu que le respect de l'anonymat de l'internaute connecté au réseau doit conduire à l'affirmation d'un nouveau principe d'effacement des

---

[826] V. Code des postes et des communications électronique, partie législative, livre I « Le service postal », titre 1er « Dispositions générales », chapitre III « Dérogations à l'inviolabilité et au secret des correspondances ».

[827] V. LOI n°86-1067 du 30 septembre 1986 relative à la liberté de communication, article 3.

[828] F.GALLOUEDEC GENUYS et H.MAISL, Le secret des fichiers, Institut français des sciences administratives, cahier n°13-1976, Paris : éditions Cujas, 1976, 328 pp

[829] KAYSER Pierre, La protection de la vie privée par le droit, Protection du secret de la vie privée, 3e éd., Paris : Économica, Aix-en-Provence : PUAM, 1995, 605pp.

[830] V. Directive 1997/66/CE du Parlement européen et du Conseil du 15 décembre 1997, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, article 5 « Confidentialité des communications ». Cette directive a été abrogée par la mise en œuvre du paquet télécom en 2002 (V. directive 2002/58/CE)

[831] F.GALLOUEDEC GENUYS et H.MAISL, Le secret des fichiers, *op.cit.*, p.4.

[832] "*Confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information*", cf. l'article "confidentiality" sur le site en.wikipédia.org/

[833] Tel un « *breach of contract* ».

[834] L'exemple de cette différence se retrouve en droit français qui pose le principe du secret des lettres missives confidentielles, que l'on distingue de l'inviolabilité ou secret de la correspondance. Le « confidentiel » renvoie à la volonté de l'un des deux correspondants, qui entend que le contenu de la lettre, une fois celle-ci ouverte, ne soit pas divulgué à des tiers par son correspondant. V.KAYSER Pierre, « Le principe du secret des lettres confidentielles et ses rapports avec le principe de droit public de la liberté et de l'inviolabilité de la correspondance », *in Mélanges Pierre Voirin*, Paris : LGDJ, 1966, p.437-465.

données révélant sa navigation sur le réseau **(§1).** Dès lors, dans un second temps, seront étudiées les procédures permettant l'interception de telles données **(§2).**

§1) L'affirmation d'un principe d'effacement des données révélant la navigation de l'internaute

423. ***Plan.*** L'objectif de sauvegarde de l'anonymat de l'internaute permet de délimiter l'objet de la protection **(A)** ce qui permet de considérer comment celle-ci peut être mise en œuvre à travers un principe d'effacement des données révélant les requêtes de l'internaute le temps de sa connexion **(B).**

A] La délimitation de l'objet de la protection

424. ***Plan.*** Il sera vu que la visualisation des adresses IP des sites demandés au point d'accès au réseau **(1)** tout comme les journaux de connexion des moteurs de recherche et l'historique des navigateurs web **(2)** permettent d'identifier l'internaute à son insu.

1) Les données de navigation collectées au point d'accès au réseau

425. **La mise à disposition d'un point d'accès.** C'est au point d'accès au réseau que sont réceptionnées les réponses aux requêtes d'un internaute. Ainsi à la manière d'un facteur qui peut relever les adresses des expéditeurs des correspondances adressées à un particulier, celui qui fournit un accès au réseau visualise les adresses des sites qui souhaitent accéder au point d'accès qu'il met à disposition. C'est en fonction de cette logique de mise à disposition d'un accès qu'il faut raisonner ; ce serait une erreur de limiter la visualisation de telles données au FAI proprement dit. Il faut considérer que toutes les personnes qui mettent techniquement à disposition un accès sont à même de visualiser l'usage qui en est fait.

Ainsi alors qu'à partir d'un point d'accès au réseau mondial, un réseau local peut être créé, l'administrateur-réseau est également à même de relever les adresses IP des sites visités par les utilisateurs de celui-ci. Le gérant d'un cybercafé ou l'administrateur d'un réseau plus étendu comme celui d'une université ou d'une entreprise peuvent ainsi suivre la navigation parmi les sites du web d'un individu auquel ils fournissent un accès.

426. **L'identification à son insu de l'internaute connecté**. Or il faut noter que le relevé des adresses IP des sites demandés permet d'identifier la personne derrière son ordinateur.

Dans le cadre d'un réseau domestique, l'adressage privé se fait automatiquement. Ainsi le FAI ne peut dissocier les choix de connexions opérées au même moment par deux internautes à partir du point d'accès au réseau qu'il met à disposition de l'abonné. Toutefois alors que l'étendue du réseau se restreint aux personnes ayant accès au

domicile de l'abonné, si le FAI relève les adresses des sites visités, il peut identifier les personnes connectées. En effet plus les données se multiplient, plus des profils d'utilisation du réseau se dessinent. On retrouve ce principe dans la technique statistique alors que les instituts de statistiques ou de sondages s'interdisent de descendre en-dessous d'un certain seuil afin d'éviter le retour d'indentification par le biais d'une caractéristique rare[835].

Dans le cadre d'un réseau local plus étendu, la dissociation des connexions par un adressage privé permet d'associer à chaque connexion individuelle une liste des sites visités qui établit un profil de connexion. Ce profil, à mesure que les données sont compilées, peut facilement être associé à une identité civile alors que le sous- réseau vise une communauté définie, comme les étudiants d'une université ou les salariés d'une entreprise, et que le point d'accès renvoie nécessairement à un périmètre physique de connexion restreint.

2) Les données de navigation collectées par les moteurs de recherche et les navigateurs web

427. **Les mots-clefs renseignés auprès d'un moteur de recherche.** En considération de la masse d'informations mises en ligne sur le web et grâce à l'ordonnancement qui en est fait par les moteurs de recherche, c'est toute pensée ou question d'un individu qui trouve à se matérialiser dans la saisie par celui-ci d'un mot-clef dans la barre de recherche de tels services. Comme le souligne John Batelle dans son livre *La révolution Google,* le moteur de recherche constitue la « *base de données de nos intentions* »[836].

---

[835] Ainsi un FAI peut relever les adresses des sites visités comme tels lors d'une session de connexion au réseau : adresse IP du site « Lemonde.fr », adresse IP du site de vente en ligne «Amazon», adresse IP du site «forum-penal.dalloz.fr/», adresse IP du site « puteaux.fr », adresse IP du site « twilight-France.blogspot.fr », adresse IP du site « justinbiebermusic.com », adresse IP du site de vente en ligne «Amazon».

La navigation est celle associée au point d'accès. On ne peut la dissocier suivant les différents utilisateurs qui pourraient utiliser le point d'accès au réseau au même moment. Dans l'exemple donné, on serait tenté de penser que plusieurs personnes se connectent au même moment, alors que l'on pourrait distinguer les requêtes vers le site du journal Le Monde, le forum pénal Dalloz et le site de la ville de Puteaux de celles vers le blog consacré à Twilight et le site officiel de Justin Bieber. Ce ne peut être qu'une supposition basée sur des critères subjectifs, la lecture du Monde et d'un forum Dalloz n'empêchant pas une passion ou une simple curiosité pour Justin Bieber, artiste ayant en son temps recueilli le plus de vues sur You Tube. Cette supposition peut toutefois s'affiner à mesure des différentes connexions au point d'accès qui révèlent des profils de navigation.

[836] BATELLE J., *La révolution Google,* Paris : Eyrolles, 2006, p.1. Ainsi le premier P.D.G de *Yahoo,* Tim Koogle interviewé par J.Batelle, se souvient comment la société a vite réalisé la valeur des clics de ses utilisateurs : « *Les gens se connectaient à nos serveurs et laissaient des traces. Nous pouvions savoir ce qui comptait sur Internet jour après jour » (La révolution Google, op.cit.* p.52). En 2001 Google publie son premier « Zeitgeist » (« esprit du temps » en allemand) un classement annuel des recherches dans le monde et par pays qui permet de visualiser les tendances de recherche d'une population. *Google* a depuis créé *Google Trends* un service dédié qui organise la mise à disposition de ces tendances de recherches auprès de ses services selon un nombre importants de critères. V. le site www.google.com/trends/ et pour les résultats de l'année 2014, www.google.fr/trends/topcharts?date=2014. Par ailleurs *Google* fait commerce de résultats de recherche plus spécifiques encore auprès d'entreprises qui souhaitent optimiser la pénétration de leurs services. Ainsi, dans son émission du dimanche 22 février 2015, le magasine « Capital », diffusé sur M6, intitulé « *Pâtisserie et chocolat, les millions d'une passion*

Dès lors une telle base de données permet d'identifier des internautes naviguant anonymement derrière leur écran. Ainsi en 2006 une fuite de 20 millions de requêtes[837] des utilisateurs du moteur de recherche *AOL* a révélé la possibilité d'identification de telles données[838]. Des outils d'analyse spécialisés ont fait apparaître que cette identification devenait possible à partir de la compilation de 200 requêtes[839] ; des journalistes ont réussi à identifier des individus et à les contacter[840].

Ainsi la problématique, comme le souligne le groupe dit du « G29 » dès 2008, est celle d'une « *anonymisation* » irréversible des données que de telles entreprises du web, *Google* en tête, collectent. Toutefois ce procédé implique de nombreuses opérations de la part du moteur de recherche[841], qui de fait ne seraient pas utiles si les données révélant les choix de navigation de l'internaute n'étaient pas conservées en premier lieu.

428. **Les données collectées par les outils de navigation.** L'accès au web nécessite d'ouvrir un logiciel spécifique appelé navigateur[842]. Les plus connus sont « *Microsoft Internet Explorer* » « *Opéra* », « *Firefox* », « *Safari* » ou encore « *Google Chrome* ». Ils permettent de visualiser les documents mis en ligne et de naviguer entre eux. Puis, alors que les possibilités permises par le web se développent, ils permettent d'accéder aux différents services proposés sur cette nouvelle interface de communication[843]. Or tous les logiciels de navigation proposent une fonction dite « Historique » qui renseigne sur les choix de navigation. Ainsi sont enregistrés tous les noms de domaine des sites visités à chaque connexion. Ces données sont conservées pendant une longue durée et classées selon un ordre chronologique ce qui

---

très gourmande », montre comment les dirigeants d'un atelier de cours de cuisine achètent auprès de *Google* le classement des requêtes de recettes de desserts pour orienter l'offre de leurs tout nouveaux cours de pâtisserie.

[837] Ce qui correspond à trois mois de recherche de 658 000 utilisateurs.

[838] V. la démonstration de Guillaume PIOLLE, chercheur en informatique, enseignant-chercheur à Supélec, en date du 7 février 2014, intitulée *Protection de la vie privée et des données à caractère personnel, Partie 2-La sécurité informatique au service de la vie privée*, disponible en ligne en version pdf à cette adresse, http://guillaume.piolle.fr/doc/matisse2.pdf, p. 44 à 47.

[839] V. L'émission « L'atelier numérique » diffusée sur BFM radio, le 1er mars 2007.

[840] V. L'article du New-York Times qui identifia une retraitée et publia le résultat de son enquête en accord avec l'intéressée. BARBARO M. et T. ZELLER, « A face is exposed for AOL searcher n°4417749 », *The New York Times*, édition du 9 août 2006.

[841] De fait l'association de l'adresse IP de la connexion et de la liste mots clefs tapés et des clics vers les sites visités permet une identification indirecte. Le forum des droits sur l'internet précise que même en tronquant l'adresse IP de son octet final et en ne gardant trace donc que de la mention du fournisseur d'accès, la personne derrière son ordinateur peut être identifiée si à cette indication de fournisseur sont associées les mots-clefs de requêtes. V. : Forum de droits de l'Internet, *Recommandation Publicité ciblée sur internet*, en date du 8 mars 2010, p.38.

[842] Le terme « navigateur » est inspiré du nom du navigateur phare au démarrage d'internet en 1995 : *Netscape Navigator*. En anglais le terme est « browser » ; on a vu également apparaître les dénominations « fureteur » ou « butineur » ou encore « explorateur » inspiré d'*Internet Explorer*. En France la Direction Générale à la langue française et aux langues de France (DGLFLF) recommande les termes de « logiciel de navigation » ou de « navigateur » (V. : JO du 16/03/1999, et la saisie du terme « navigateur » dans la base de données Franceterme, www.culture.fr/franceterme). V. également l'entrée « navigateur web» sur le site fr.wikipédia.org

[843]Ainsi, aujourd'hui pour envoyer un courriel, il est usuel d'ouvrir son navigateur pour accéder à un service de messagerie en ligne tel que « *Gmail* ». Avant il était d'usage d'utiliser un logiciel spécifique de courrier électronique tel *Microsoft outlook* par exemple.

permet à l'utilisateur de retrouver un site qu'il a visité et qu'il souhaiterait consulter à nouveau.

Dès lors de la même manière que s'agissant des adresses IP visualisées par le FAI et des mots-clefs renseignés à disposition du moteur de recherche, le navigateur, via cette fonction d'historique et la compilation des données de navigation qu'elle met en œuvre, peut considérer l'identité de l'individu à l'origine de chaque connexion.

B] La mise en œuvre du principe d'effacement des données

429. **L'effacement des données révélant les choix de navigation de l'internaute**. Il est important de souligner ici que la logique n'est pas de garantir la confidentialité s'agissant de données qui seraient dès lors conservées. Il s'agit bien, à l'inverse, d'affirmer que les données révélant la navigation de l'internaute le temps de sa connexion, que ce soit les adresses IP des sites visités ou les mots-clefs de recherche renseignés, doivent être effacées. Elles seront interceptées le cas échéant dans le cadre de procédures strictes.

Il a été vu que cette obligation d'effacement apparaît dans la législation visant les opérateurs de communications électroniques mais d'une manière si peu claire qu'il est proposé de la formuler autrement à travers une obligation générale d'effacement des données de navigation à la charge de toute personne attribuant une adresse IP **(1).**

S'agissant des données collectées par les moteurs de recherche et les navigateurs web cette logique d'effacement apparaît beaucoup plus difficilement dans les régimes existants visant les données qu'ils collectent alors que ces entreprises du web arguent de la nécessité fonctionnelle pour eux d'analyser les données de navigation de leurs internautes. Il faut dès lors, s'agissant de ces fonctionnalités, considérer un régime spécifique qui toutefois doit viser comme objectif l'effacement des données alors que la puissance des algorithmes permet une analyse de plus en plus immédiate et que les usages de navigation évoluent (**2)**.

1) L'obligation d'effacement à la charge de toute personne attribuant une adresse IP

430. **La définition d'une obligation générale**. Il doit être garanti à l'internaute que ses choix ne seront pas visualisés quelque soit l'accès qu'il utilise. Le régime de l'effacement des adresses IP des sites visités ne doit plus ressortir de celui visant les opérateurs de communications électroniques qui mettent structurellement en œuvre la connexion sur le réseau public. Il s'agit d'affirmer un principe général d'effacement qui s'inscrit dans le prolongement des secrets de communication : personne n'a à connaître de la navigation de l'internaute le temps de sa connexion.

Ce principe doit être immédiatement compréhensible par tous ; l'individu doit être assuré que quand il se connecte au réseau ses choix de connexions ne peuvent pas être connus de la personne qui lui permet cet accès. Qu'il se connecte depuis son domicile, qu'il entre dans un cybercafé, qu'il se connecte au spot wifi de son université ou de son lieu de travail, le principe est l'effacement des données pour garantir sa liberté d'accès.

Il est ainsi proposé de le formuler ainsi : toute personne attribuant une adresse IP valide à une connexion doit être soumise à une obligation d'effacement des adresses IP requises à partir de ce point. Une obligation qui à l'instar du secret des correspondances pourrait être rendue effective par la définition d'une sanction pénale, prolongée par « *la sanction processuelle, à la portée générale, du non-respect du principe de loyauté de la preuve* »[844].

431. **La possible surveillance de l'internaute.** Par ailleurs, ce principe d'effacement n'empêche pas la mise en œuvre d'une interception de telles données mais celle-ci ne peut intervenir qu'à rebours de cette prescription générale. La logique ici est celle de la mise en œuvre d'une surveillance. Disant cela les limites des exceptions à l'effacement des données apparaissent plus clairement.

Le régime d'interception ne peut ressortir que d'un rapport de contrôle entre celui qui met à disposition l'accès et l'internaute. Seul celui-ci permet d'envisager un accès aux données qui renvoie aux faits et gestes de l'internaute. Une surveillance qui, si elle n'est pas mise en œuvre par les pouvoirs publics, doit nécessairement être portée à la connaissance de l'individu.

2) Le contenu du régime visant les moteurs de recherche et les navigateurs web

432. ***Plan***. Eu égard au caractère identifiant des données à leur disposition, il est proposé d'affirmer d'une part que les données de requêtes à disposition d'un moteur de recherche soient supprimées définitivement une fois la communication achevée **(a).** D'autre part, il est proposé de soumettre la fonctionnalité d'historique des navigateurs web à un régime dit « d'opt-in » dès lors que par défaut toute navigation devrait être privée **(b).**

[844] A. LEPAGE, *Libertés et droits fondamentaux à l'épreuve de l'Internet,* Paris : Litec, 2002, p. 39.

a. L'effacement des données de requêtes à disposition des moteurs de recherche

433. **Les crispations autour du régime de conservation des journaux de connexion des moteurs de recherche**. Il n'est pas de législation imposant une limite à la conservation des données de connexions à la disposition des moteurs de recherche ; si ce n'est en application de l'encadrement des données personnelles, que celle-ci soit proportionnée à la finalité poursuivie.

Or en 2007, des crispations se font sentir entre le groupe dit du « G29 » et les moteurs de recherche notamment *Google*. Les entreprises entendent les préoccupations des Cnil européennes mais arguent de la nécessité d'améliorer leur algorithme, de la lutte contre la fraude au clic et de la lutte contre les spams[845]. Néanmoins, là où aucune limite n'est posée, Google et Microsoft consentent d'abord à réduire la durée de conservation de leurs logs à 2 ans, puis à 18 mois. *Yahoo* et *Aol* décident d'une durée de 13 mois. En 2008, le « G29 » considère que les données devraient toutefois être effacées dès que possible et au plus tard 6 mois après leur production[846] ; ce dont actent les moteurs de recherche dans un premier temps avant de se rétracter arguant des nécessités de leurs services.

434. **La difficile mise en balances des intérêts en présence**. La problématique est alors de considérer les intérêts en présence alors que la collecte des données de requêtes participe du fonctionnement du moteur de recherche mais que par ailleurs ces données portent atteinte à l'intimité de la personne. La CNIL en 2011 devant la résistance des moteurs de recherche réaffirme la nécessité d'un délai d'effacement qu'elle fixe à 6 mois et demande à ce que soit recueilli le consentement de l'utilisateur pour une conservation plus longue[847].

Selon une toute autre logique, le 23 juin 2010, une déclaration écrite, qui n'a pas de valeur contraignante, est adoptée par le Parlement européen[848], non sans remous[849], qui « *invite le Conseil et la Commission à mettre en œuvre la directive 2006/24/CE aux moteurs de recherche pour contrer avec rapidité et efficacité, la pédopornographie et le*

[845] « Google ramène la durée de conservation des données utilisateurs à 18 mois », article mis en ligne le 13 juin 2007, par Vincent Delfau, sur le site lemondeinformatique.fr.

[846] Groupe de travail « article 29 » sur la protection des données, Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, adopté le 4 avril 2008.

[847] Actu. CNIL du 9 mai 2011.

[848] Sur la procédure d'adoption d'une déclaration écrite, voir article 123 du règlement du Parlement européen.

[849] « Les eurodéputés favorables à l'enregistrement des recherches web », Le Monde.fr, article mis en ligne le 21/06/10.

harcèlement sexuel en ligne »[850]. Ainsi, certains députés européens souhaiteraient que tout comme les opérateurs de communications électroniques avec leurs données relatives au trafic, les moteurs de recherche ainsi que d'autres services en ligne[851], soient soumis à une obligation minimale et maximale de conservation des fichiers journaux.

Il faut bien distinguer ce souhait de celui de la CNIL et du G29. La logique de la protection des données personnelles n'oblige pas à la conservation des « logs », l'idéal étant que ceux-ci soient effacés immédiatement ; mais si conservation il y a, il faut la limiter. Les députés européens qui ont signé la déclaration souhaitent, en revanche, que les moteurs de recherche et autres sites de contenus générés par les utilisateurs soient soumis à une durée de conservation définie[852] et à des modalités d'accès justifiées par un but de lutte contre des infractions dont la gravité ne saurait être remise en question. Toutefois cet accès ne peut être alors qu'il ne peut s'agir d'une manière générale de conserver l'ensemble des données de connexion des individus pour y accéder le cas échéant, comme l'a souligné la CJUE en invalidant la directive dite de « *retention data* »[853].

Dans les deux cas, la limite d'un régime visant la conservation de données apparaît. Il convient de prôner un régime d'effacement à l'heure où la puissance des algorithmes est démultipliée.

435. **La mise en œuvre de l'obligation d'effacement à l'égard des moteurs de recherche.** Il faut affirmer que les moteurs de recherche doivent effectivement être soumis à la même obligation que les opérateurs de communications électroniques, et qui devrait s'appliquer *in fine* à toute personne ayant techniquement accès aux données révélant les requêtes de l'internaute : toutes les données révélant le contenu des informations consultées doivent être effacées une fois la communication achevée.

D'une part il faut constater que l'évolution des moteurs de recherche montre qu'un tel service peut être performant sans collecter de données sur ses utilisateurs à l'instar du moteur historique arguant d'une telle politique « *Duckduckgo* », concurrencé aujourd'hui par d'autres modèles de ce genre[854]. D'autre part, si l'on peut considérer

[850] V. cette déclaration disponible sur le site du Parlement européen : http://www.europarl.europa.eu/activities/plenary/writtenDecl/wdFastAdopted.do;jsessionid=1290240BFB9F06C02584F34533D59D2D.node1?language=FR

[851] GIRARDEAU Astrid, « Conservation des données par les moteurs de recherche, l'Europe s'agite », sur le site « Owni, digital journalism, sociétés pouvoirs et cultures numériques », le 16/06/10. http://owni.fr/2010/06/16/la-conservation-des-requetes-par-les-moteurs-de-recherche/#

[852] Les durées seraient alors de 6 mois minimum et 2 ans maximum si leur était appliquée la directive 2006/24/CE.

[853] CJUE 8 avr. 2014, Digital Rights Ireland c/Ireland C293/12 et C594/12. V. *supra* n°401

[854] L'entreprise *DuckDuckGo* a été créée en 2008 par l'entrepreneur Gabriel Weinberg. On citera également le moteur français *Qwant* ou encore *Yippy*.

l'enjeu pour les moteurs de recherche, services commerciaux avant tout, d'assurer la pérennité de leur modèle, il faut envisager aujourd'hui que le développement de la technologie puisse permettre une analyse en temps réel des données et un processus d'anonymisation efficient alors qu'il ne peut s'agir de pouvoir individualiser les requêtes via une adresse IP ou un cookie. Il doit être permis aux moteurs de recherche de considérer des tendances de recherche mais dans un temps très limité. En revanche, ils ne peuvent constituer des gisements de données qui comme l'image l'indique, puissent être exploités à des fins diverses et propres aux entreprises qui les détiennent en vue de développement de services futurs.

Ce principe d'effacement des données de requêtes des moteurs de recherche doit trouver son prolongement dans un régime « *d'opt-in* » s'agissant de toute fonction d'historique de navigation.

b. La mise en œuvre d'un régime « d'opt-in » à toute fonction d'historique de navigation

436. **Le développement de l'option dite de « navigation privée ».** Il est à noter que suite à l'affaire Snowden[855], les différents navigateurs du marché ont commencé à proposer une option de « navigation privée »[856]. Il s'agit d'une fonctionnalité qui permet que l'historique de navigation ne soit pas enregistré. Les informations que l'internaute pourrait saisir dans un formulaire, ou les cookies visant son authentification à des services ne sont pas non plus enregistrés dans le terminal utilisé. Ainsi sa navigation ne laisse aucune trace sur l'ordinateur, et quelqu'un qui se connecterait après lui ne peut considérer ni ses pérégrinations, ni ses éventuels identifiants de connexion à certains services.

Il faut souligner comme le fait le navigateur de Google, « *Chrome* », que « *seul Chrome n'enregistre pas les sites que vous consultez. D'autres sources continuent d'avoir accès à votre activité de navigation, notamment : votre fournisseur d'accès à Internet, votre employeur (si vous utilisez un ordinateur professionnel), les sites web*

459 Du nom de ce jeune informaticien, employé de la NSA qui, à l'été 2013, a révélé le fonctionnement de divers programmes de surveillance électronique de cette agence de renseignement américaine, qui enregistraient les faits et gestes de l'ensemble de la population mondiale, via les données de navigation et les données de contacts notamment. L'un des programmes s'intitulant « *Prism* », l'affaire est aussi désignée comme le scandale « *Prism* ». V. le film « Snowden» du réalisateur américain Olivier Stone, sorti à l'automne 2016.

856 Ainsi sur le navigateur *Mozilla*, dans le Menu (symbolisé par trois barres horizontales en haut à droite de la fenêtre du navigateur), il faut sélectionner « fenêtre privée », une nouvelle fenêtre s'ouvre alors qui porte un entête figurant un masque de couleur violette, ce qui permet de la distinguer d'une fenêtre qui enregistre l'historique de navigation. Sur le navigateur Chrome, dans le menu (symbolisé par trois points en haut à droite de la fenêtre du navigateur), sélectionnez « nouvelle fenêtre de navigation privée », une nouvelle fenêtre s'ouvre alors de couleur noire ce qui la distingue de la navigation traditionnelle.

Il faut noter par ailleurs le développement d'une nouvelle offre de navigateur dont la fonctionnalité première est de permettre une navigation privée. Ainsi du navigateur créé par quatre étudiants en informatique suisses, *Snowhaze* qui entre autres protège des scripts de poursuites mis en œuvre par les sites Web et ne conserve pas par défaut l'historique de navigation de ses utilisateurs. A l'inverse il faut activer une option si l'on souhaite conserver l'historique. V. snowhaze.com

que vous consultez. »[857]. En effet seul le navigateur est concerné par cette navigation privée, la mise en œuvre d'une connexion continue à produire des données qui peuvent être collectées au point de départ de la communication par le FAI ou l'administrateur réseau d'une entreprise ou d'un quelconque sous-réseau, et au point d'arrivée par les sites web[858].

Mais de fait cette navigation enregistrée par le navigateur doit ressortir du même régime. Il ne s'agit pas de mettre son secret à la charge de l'individu.

437. **Le choix d'un régime « *d'opt-in* » à toute fonction d'historique.** Le relevé de la navigation d'un internaute ne peut être s'il n'a pas donné son accord à celui-ci. Ainsi le régime doit être non pas celui d'une option de navigation dite « privée » mais celui du choix de conservation de ses données le temps de sa connexion. La logique ne peut être pour l'internaute de décider de se cacher le temps d'une consultation. Si cette fonction d'historique est utile à l'internaute, il doit pouvoir paramétrer en ce sens son navigateur pour considérer à posteriori les sites qu'il a visités.

Disant cela la désuétude d'une telle fonction apparaît à l'heure du web applicatif et alors que les outils pour mémoriser un site ou conserver une page du web ont évolué. En effet à l'époque des débuts d'internet la navigation se faisait réellement grâce aux liens hypertexte, d'où la dénomination de « *toile d'araignée* » car il était difficile d'envisager de se rendre d'une page éloignée à une autre sans une navigation à travers différents nœuds du réseau. Ainsi les premières navigations s'apparentaient à un véritable « *surf* » ; un document portait l'internaute vers un autre ; et le recours à l'historique de navigation était fréquent pour retrouver un site consulté. La recherche d'informations sur le web ne se pratique plus comme cela aujourd'hui alors que l'internaute est actif : il peut enregistrer ses favoris, enregistrer des pages web dans des applications telles « *pocket* » pour les lire ultérieurement, faire sa veille informationnelle en tweetant des informations dont il souhaite se souvenir.

[857] V. la page d'activation de l'option de navigation privée de Google Chrome. Mozilla délivre la même information : « *La navigation privée ne vous rend pas anonyme sur Internet. Votre fournisseur d'accès à Internet ou votre employeur peuvent toujours connaître les pages que vous visitez.* ».

[858] Ainsi il est intéressant de noter que quand un service de l'entreprise Google, tel le moteur de recherche, est utilisé dans le cadre d'une fenêtre de navigation privée, un bandeau apparaît qui s'intitule « *Rappel concernant les règles de confidentialité Google* » et qui permet de cliquer pour en prendre connaissance. Google rappelle ainsi aux internautes désireux de protéger leur vie privée puisqu'actuellement en train d'utiliser une fenêtre de navigation privée, les choix qui s'offre à lui s'agissant du moteur de recherche : « *modifier les paramètres recherche, modifier les paramètres des annonces, modifier les paramètres Youtube* ».

438. **Un principe d'effacement d'ordre public et non un droit d'accès garanti à l'internaute.** Ainsi il faut condamner la logique de la conservation des données par défaut qui renvoie à un raisonnement faux sur le contrôle ultérieur que les internautes en auraient. C'est la politique de Google depuis plusieurs années déjà, qui inaugurait son « *Dashbord* » en 2009 et qui en 2016, en anticipation de l'entrée en vigueur du RGPD a mis en place la fonction « *MyActivity* » qui permet de visualiser l'historique des recherches notamment mises en œuvre via son moteur de recherche, recherches qui sont individualisées dès lors que l'internaute est détenteur d'un compte *Gmail*.

Ainsi le site *myactivity.google.com* permet une fois renseignée son adresse *Gmail* et le mot de passe associé, de prendre connaissance ou plutôt d'appréhender concrètement l'enregistrement par Google de toutes les recherches effectuées sur le web alors que l'internaute était logué dans le cadre de la connexion à son compte de messagerie.

Google souligne que cette politique vise à permettre à l'internaute de contrôler son activité puisque chaque trace de recherche peut être supprimée. L'entreprise californienne répond ainsi aux exigences de droit d'accès et de suppression de la protection visant les données personnelles. En réalité cette position ne peut être. Le principe d'effacement des choix de navigation doit être d'ordre public. Il doit s'imposer à tous et ne pas relever de la responsabilité de l'individu.

Disant cela la logique d'une filature numérique apparaît qui ressort de l'interception de données qui ne sont pas par principe conservées. Il ne s'agit pas d'accéder aux données mais de suivre les choix d'un internaute en particulier, de manière limitée dans le temps, dans le cadre d'une surveillance légitime.

§2) L'encadrement de l'interception de telles données

439. **La surveillance d'un internaute**. Le vocabulaire Cornu définit la surveillance comme l' « *action de veiller sur une personne ou une chose dans l'intérêt de celle-ci, ou de surveiller une personne ou une opération pour la sauvegarde d'autres intérêts* »[859]. La surveillance fait ainsi apparaître une logique de contrôle : il faut contrôler les faits et gestes d'un individu pour le protéger ou protéger des intérêts tiers. Ainsi, transposée au réseau, la problématique est de considérer quels intérêts légitimes peuvent fonder le suivi de la navigation d'un internaute en particulier.

[859] V. l'entrée « *surveillance* », in CORNU G., Association Henri Capitant, Vocabulaire juridique, 11ème éd., Paris : PUF (Quadrige).

D'emblée il faut souligner que le raisonnement n'est pas celui d'une mise en balance du droit à la vie privée à travers le prisme de la protection des données personnelles ; l'enjeu n'est pas la maitrise de l'individu sur ses données. A l'instar du secret des correspondances, la confidentialité de la navigation se défend bien toute seule[860], une fois les contours de son régime définis qui pénalise la conservation des données de requêtes de l'internaute.

Dès lors il s'agit de considérer les conditions de la mise en œuvre d'une filature numérique qui intervient comme un fait justificatif nécessaire à la sauvegarde d'intérêts définis.

440. ***Plan***. Ces intérêts peuvent être de deux ordres. D'une part une surveillance sécuritaire peut être mise en œuvre à l'instigation de l'État en vue de la sauvegarde de l'ordre public **(A).** D'autre part une surveillance hiérarchique est légitime qui procède du pouvoir de contrôle de celui qui met à disposition un système d'information à des utilisateurs spécifiés **(B).**

A] Le régime de la surveillance sécuritaire visant la sauvegarde de l'ordre public

441. **Les régimes de suivi de la navigation d'un internaute prévus par la loi.** La législation française autorise les autorités publiques à connaître des choix de navigation d'un internaute dans le cadre de deux techniques différentes qui font l'objet de deux régimes différents.

D'une part il peut être requis des opérateurs de communications électroniques qu'ils préservent le contenu des informations consultées au point d'accès de l'un de leurs abonnés ; une réquisition opérée sous contrôle d'un juge qui ne peut intervenir que dans le cadre d'une opération de police judiciaire **(1).** D'autre part une filature numérique peut être mise en œuvre à la fois par les autorités judiciaires et administratives qui sont autorisées dans le cadre d'une procédure stricte à capter les informations telles qu'elles s'affichent sur l'écran de l'ordinateur **(2).**

1) La préservation par les opérateurs de télécommunications du contenu des informations consultées

442. **Une procédure de réquisition nécessaire à la recherche, au constat et à la poursuite des infractions pénales**. En 2003, la loi pour la sécurité intérieure[861] crée l'article

[860] Pour reprendre une expression du professeure Lepage. V. : A. LEPAGE, *Libertés et droits fondamentaux à l'épreuve de l'Internet,* Paris : Litec, 2002, p.40.

[861] Loi n°2003-239 du 18 mars 2003, JORF du 19 mars 2003, n°66, p. 4761-4789, article 18.

60-2 du Code de procédure pénale (CPP). L'alinéa 2 de cet article permet dans le cadre de l'enquête de flagrance, à un officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, de requérir « *des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs. ».*

La loi dite « Perben II » du 9 mars 2004[862] va étendre cette possibilité de réquisition aux opérations menées pendant l'enquête préliminaire grâce à l'article 77-1-2 du CPP, et la rendre licite également dans le cadre de l'instruction grâce à l'article 99-4 du même code.

443. **L'autorisation nécessaire d'un juge**. Dans ces trois hypothèses, la mise en œuvre d'une telle préservation de données de contenu visant les informations consultées le temps des connexions au réseau d'un abonné ne peut être mise en œuvre qu'avec l'accord d'un juge. Dans le cas de l'enquête de flagrance et de l'enquête préliminaire, l'officier de police judiciaire ne peut agir de son propre chef mais bien sur réquisition du procureur de la République, après autorisation du le juge des libertés et de la détention. Dans le cadre de l'instruction, l'officier de police procède avec l'autorisation expresse du juge d'instruction.

2) La captation des données informatiques telles qu'elles sont stockées dans un système informatique ou s'affichent sur l'écran de l'ordinateur

444. ***Plan.*** La captation des données informatiques telles qu'elles s'affichent sur l'écran de l'ordinateur et qui peuvent donc révéler les sites visités par l'internaute peut procéder d'une investigation judiciaire dans le cadre de la lutte contre la criminalité et la délinquance organisée **(a)** ou d'une technique de renseignement dans le cadre de la défense de la sécurité intérieure **(b).**

[862] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF du 10 mars 2004, n°59, p.4567-4637, article 80.

a. Les dispositions visant les investigations judiciaires dans le cadre de la lutte contre la criminalité et la délinquance organisée (Section VI. Bis- 706-102-1 et suiv., titre XXV, Livre IV. CPP)

445. **De la procédure applicable à la criminalité et à la délinquance organisée.** En 2004 la loi dite « Perben II »[863] ajoute dans le CPP, au livre IV « *De quelques procédures particulières* », un livre XXV qui vise spécifiquement « *De la procédure applicable à la criminalité et à la délinquance organisée* ». Ce livre s'ouvre sur un article 706-73 qui qualifie dix-neuf infractions pouvant faire l'objet d'une telle procédure.

En 2011, la loi dite « LOPPSI 2 » introduit dans le chapitre 2 de ce titre XXV, une nouvelle section « 6-bis "*De la captation des données informatiques" »*[864]. Une nouvelle technique est introduite au stade de l'information qui consiste « *à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels* ». Depuis la loi 2016-731 « *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale* »[865], cette technique est permise au stade de l'enquête visant de telles infractions relatives à la criminalité et à la délinquance organisée.

446. **L'autorisation nécessaire d'un juge.** Ainsi l'article 706-102-1 du CPP permet sa mise en œuvre par les officiers de police judiciaire au stade de l'enquête. Toutefois cela se fait à la requête du procureur de la République, après autorisation par ordonnance motivée du juge des libertés et de la détention. Au stade de l'information, l'article 706-102-2 du CPP énonce que le juge d'instruction autorise après avis du procureur de la République, les officiers de police judiciaire à mettre en œuvre un tel procédé.

L'article 706-102-3 définit les conditions de la mise en œuvre d'une telle captation de données, et notamment sa durée qui ne peut excéder un mois si ce procédé est mis en œuvre au stade de l'enquête, et quatre mois s'il est mis en œuvre dans le

[863] [863] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF du 10 mars 2004, n°59, p.4567-4637, article 1er.

[864] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF du 15 mars 2011, n°62, p.4582, article 36.

[865] LOI no 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF du 4 juin 2016, Texte 1 sur 119, article 5.

cadre d'une information judiciaire. L'article 706-102-4 précise que le magistrat qui a autorité une telle captation peut à tout moment ordonner son interruption.

b. Les dispositions visant cette technique de renseignement dans le cadre de la défense de la sécurité intérieure (article 853-2 du CSI).

447. **Une technique de recueil de renseignement**. En 2015, la loi relative au renseignement[866] introduit dans le Code de la sécurité intérieure, dans le livre VIII « Du renseignement », au niveau du titre V « *Des techniques de recueil de renseignement soumises à autorisation* », un nouveau chapitre 3 intitulé « *De la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques* ».

Celui-ci comporte un article L853-2 dont le 2° permet aux agents des services de renseignement spécialement habilités : « *2° D'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques.* ». Ainsi un tel agent peut concrètement considérer la navigation d'un individu connecté depuis un ordinateur surveillé.

448. **Une technique soumise à autorisation**. Cette opération obéit au régime général entourant toute technique de renseignement prévu par ce Livre VIII de la sécurité intérieure. Comme le rappelle l'article 801-1, c'est un régime de liberté publique. Les finalités sont précisées à l'article 811-3. Toute opération est autorisée par le Premier ministre après avis de la CNCTR en application de l'article 821-1.

Par ailleurs par dérogation au délai général applicable à de telles opérations qui est de quatre mois, la mise en œuvre d'une telle captation ne peut être mise en œuvre que pour une durée maximale de deux mois[867]. Les dispositifs techniques mentionnés au I du présent article ne peuvent être utilisés que par des agents appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 dont la liste est fixée par décret en Conseil d'Etat[868].Un compte-rendu doit être adressé à la CNCTR qui peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits[869].

[866] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF du 26 juillet 2015, texte 2 sur 49.
[867] Article L8453-2,II.
[868] Article L8453-2,III.
[869] Article L8453-2,IV.

B] Le régime de la surveillance hiérarchique visant le contrôle de l'utilisateur d'un système d'information

449. **La surveillance hiérarchique**. La surveillance hiérarchique procède du pouvoir de contrôle de celui qui met à disposition un système d'information **(1).** Elle est doit être soumise à des conditions strictes **(2).**

1) Le pouvoir de contrôle sur un utilisateur

450. **Le contrôle d'un utilisateur autorisé à se connecter.** Un individu peut accéder à internet depuis sa propre connexion au réseau mondial, chez lui ou sur son téléphone mobile mais également en tant qu'utilisateur de sous-réseaux qui lui permettent cet accès comme celui mis à sa disposition par son employeur ou, pour un étudiant, par son université. L'internaute est alors autorisé à se connecter dans le cadre de tels sous-réseaux administrés qui lui fournissent un identifiant et un mot de passe définis.

Dès lors il peut accéder aux moyens informatiques mis à disposition dans les locaux et aux ressources des serveurs internes à travers un intranet mais également aux ressources extérieures, c'est-à-dire à l'ensemble du web. Il accède ainsi à un système d'information, c'est-à-dire « *un ensemble de moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications »*[870].

451. **La mise en œuvre d'un fait justificatif au principe d'effacement des données de requêtes.** Or la mise en œuvre de ce système implique une surveillance des connexions pour d'une part assurer la sécurité de celui-ci. Il faut assurer l'intégrité des données en particulier contre un effacement ou des modifications malveillantes et pour se faire considérer des schémas de connexions.

D'autre part le rapport professionnel établi entre l'entité hiérarchique qui met à disposition le système et les utilisateurs de celui-ci permet un contrôle des connexions opérées. Comme l'a souligné la Cour de cassation dans un arrêt en date du 9 juillet 2008 : «*les connexions établies par un salarié sur des sites internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors sa présence »*[871]. La distinction opérée pour les courriers électroniques de la messagerie professionnelle et les

[870] V. Charte d'utilisation des ressources informatiques de l'Université Panthéon-Assas, p.1.

[871] Cass. Soc. 9 juillet 2008, n° 06-45800, *Bull.* 2008, V., n°150. V. : CRIQUI Géraldine, « Les connexions établies par un salarié sont présumées avoir un caractère professionnel », article mis en ligne sur le 4 décembre 2008, sur le site du cejem, www. cejem.com

dossiers enregistrés sur le poste informatique qui peuvent être marqués de la mention « personnel » ne peut en effet intervenir ici.

Toutefois cette formulation qui légitime la surveillance des choix de connexions d'un salarié ou de l'utilisateur d'un réseau local apparaît maladroite en ce qu'elle semble envisager la navigation comme un ensemble de données accessibles de manière absolue à l'employeur. Or il faut distinguer ici, le support fonctionnel, les données, qui effectivement ne peuvent être dissociées suivant que les connexions sont professionnelles ou personnelles, de l'enjeu de l'accès à de telles données qui relève du suivi des faits et gestes d'un individu et qui doit ressortir d'un régime strict.

2) Les conditions de cette surveillance

452. ***Plan.*** Tout procédé de surveillance de l'utilisateur d'un réseau informatique doit être porté à sa connaissance **(a)** et être proportionné au but poursuivi **(b).**

a. L'information de l'utilisateur dans le cadre de la Charte informatique

453. **L'information de l'utilisateur s'agissant d'un dispositif de surveillance**. Si le contrôle des connexions peut se faire à l'insu de l'utilisateur, celles-ci étant présumées professionnelles, l'on peut s'interroger toutefois sur le point de savoir si ce possible accès aux choix de navigation doit être porté à la connaissance de l'utilisateur.

L'article L1222-4 du Code du travail énonce en effet que « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté à sa connaissance* ». De plus l'article L2323-47 al 3 de ce même code dispose que : «*Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés* ». Toutefois le caractère de dispositif de surveillance peut être discuté puisqu'il ne s'agit pas de mettre en œuvre techniquement une collecte des données via un procédé technique spécial, celle-ci se réalise automatiquement par la mise en œuvre de la communication.

Toutefois ces données, comme le premier paragraphe l'a montré, relèvent d'un principe général d'effacement pour garantir la liberté d'accès au réseau de chacun. Ainsi leur conservation par exception, pour pouvoir être justifiée, doit être portée à la connaissance des utilisateurs.

454. **Le rôle de la Charte informatique**. La pratique consiste aujourd'hui à adopter dans le cadre des entreprises, des collectivités territoriales ou des établissements qui de manière

générale mettent à disposition un accès, un document communément appelé « Charte informatique » ou « Charte utilisateur » qui fixe les conditions d'utilisation des moyens et ressources informatiques mis à disposition.

Il convient dans le cadre de ces documents de faire apparaître clairement que les choix de navigation opérés à partir de la connexion authentifiée peuvent faire l'objet d'un suivi qui répond de conditions strictes ressortant de la politique de gestion des journaux informatiques.

b. Les principes devant guider la politique de gestion des journaux informatiques

455. **Le principe de proportionnalité.** La conservation des données de navigation des utilisateurs d'un réseau local doit répondre du principe de proportionnalité qui encadre la surveillance de l'employé. Il est défini à l'article L1121-1 du Code du travail qui énonce : « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir, ni proportionnées au but recherché* ».

Ainsi quand bien même les connexions sont présumées professionnelles, il ne peut s'agir pour l'employeur de conserver ces données indéfiniment, ni d'y avoir accès sans aucune limite. A cet endroit il faut différencier la logique de sécurisation du système que doit poursuivre l'administrateur réseau, de celle du contrôle de l'utilisateur mis en œuvre par l'autorité hiérarchique[872].

456. **Les droits de l'administrateur réseau, le contrôle de l'autorité hiérarchique**. L'administrateur réseau met en œuvre les journaux informatiques qui peuvent faire apparaître les URL des sites visités. Ces journaux doivent être soumis à un régime de conservation stricte qui pour les données de contenus ne peuvent excéder quelques mois[873]. L'accès à ces données doit être ponctuel et motivé par les tâches de personnes définies qui assurent la sécurité du système d'information. Ces personnes sont soumises à une obligation de confidentialité[874].

[872] Sur cette distinction, s'agissant de l'accès aux courriers électroniques des salariés, v. Cass. Soc. 17 juin 2009, n°08-40274, *Bull.* 2009, V., n°153, *Sté Sanofi Chimie c/M. Guzzi et al.* ; MAILLARD S. « L'administrateur réseau peut ouvrir les messages personnels des salariés dans le cadre de sa mission », *JCP G*, n°39, 21 sept. 2009, n°263, p.22.

[873] On rappellera que s'agissant des données d'adressage les journaux des réseaux locaux comme ceux des opérateurs de communications électroniques doivent être soumis à une durée de conservation de 1 an pour permettre l'identification de l'internaute connecté.

[874] Cass. Soc. 17 juin 2009, n°08-40.274, FS P+B, *Sté Sanofi Chimie c/M. Guzzi et al*., *op.cit.*

En revanche la chaîne hiérarchique ne saurait avoir le même accès aux données. L'employeur ne peut avoir accès à rebours aux éventuelles informations de contenus enregistrées au nom d'un individu logué. Il doit mettre en œuvre de manière ponctuelle ce contrôle : c'est-à-dire qu'il doit définir auprès de l'administrateur-réseau l'étendue des modalités de contrôle à mettre en œuvre s'agissant d'un individu spécifié, contrôle qui ne peut excéder quelques jours alors que ce qui est recherché est l'utilisation résiduelle ou non, à des fins personnelles, de la connexion mise à disposition.

Conclusion du chapitre 2ème

457. **La nécessaire refonte du régime visant les données relatives au trafic**. Il convient d'affirmer d'une part que la protection des données relatives au trafic fait aujourd'hui apparaître ses limites. La systématisation des données produites par chaque connexion au réseau n'est pas opérante ; elle ne permet pas de dissocier les différents objectifs de protection de l'individu.

Comme le titre I l'a montré, les points d'accès doivent faire l'objet d'un fichage et les adresses IP attribuées le temps de la connexion à un lieu physique de connexion doivent être conservées 1an. En revanche il faut restaurer le secret des correspondances qui doit relever d'une logique d'interception et non de conservation de données. Enfin il faut envisager deux nouveaux régimes à l'heure de la communication mobile et interactive : l'un encadrant la géolocalisation de l'individu et l'autre encadrant le suivi de la navigation de l'internaute.

458. **L'ineffectivité du régime visant la mise en œuvre d'un cookie de navigation.** D'autre part il faut mettre fin à la fiction de l'obligation de consentement pour l'internaute à la mise en œuvre d'un cookie, qui peut être de navigation, par les sites et services du web. La mise en œuvre d'un cookie ne menace pas la liberté d'accès et de navigation sur le réseau dès lors que les informations qu'il agrège sont limitées par le contexte de leur collecte. Il faut dissocier le suivi de la navigation d'un internaute parmi les pages d'un site web ou d'un service qui permet une personnalisation des services, du suivi de l'internaute le temps de sa connexion, entre les différents services du web.

Le procédé du cookie ou « témoin de connexion » est inhérent au web ; il participe de sa fonctionnalité et de son économie. La problématique ne relève pas de la protection de l'individu mais de la sauvegarde de la diversité des contenus et des offres. En réalité ce qu'il convient d'interdire est un suivi qui par ses caractéristiques même menacerait la libre-détermination de l'individu alors que ses choix le temps de sa connexion au réseau peuvent l'identifier à son insu.

459. **Le régime du secret de la navigation de l'internaute.** La centralisation des adresses IP des sites visités au point d'accès au réseau permet, au fur et à mesure que les connexions se multiplient, de découvrir qui se connecte à partir d'un point d'accès. De la même manière, les

mots-clefs de recherche tapés dans un moteur de recherche, et la navigation associée, permettent, par leur agrégation et leur individualisation via un cookie, la révélation de l'identité civile de l'internaute connecté.

Dès lors les requêtes de l'internaute le temps de sa connexion au réseau doivent faire l'objet d'un secret. Un principe d'effacement de ces données doit être affirmé qui vise non seulement toute personne attribuant une adresse IP valide à la connexion, et à même dès lors de visualiser les adresses IP des sites web requises à partir de ce point, mais également les interfaces permettant la navigation sur le web, que sont les sites de moteurs de recherche et les logiciels-navigateur comme *Chrome* ou *Mozilla*. L'option de navigation privée n'a pas de sens ; la conservation d'un historique de navigation par ces outils doit ressortir du régime de l' « *opt-in* », c'est-à-dire relever de la volonté de l'internaute.

L'accès à de telles données doit ainsi s'envisager comme une exception au principe d'effacement et ressortir du régime de l'interception qui renvoie à l'enjeu de la surveillance de l'individu. Une telle interception ne peut être que si elle vise des d'intérêts légitimes, que sont la sauvegarde de l'ordre public et l'éventuel pouvoir de contrôle qu'exerce sur l'internaute celui qui met à disposition son accès. La procédure de ces interceptions est stricte. Elles ne peuvent être que ponctuelles et intervenir pour une durée limitée. Dans le cas d'une surveillance sécuritaire visant la défense de l'ordre public, divers procédés permettent d'appréhender la navigation de l'internaute. Ils doivent être autorisés par un juge dans le cadre d'une opération de police judiciaire ou par la Commission nationale de contrôle des techniques de renseignement dans le cadre d'une opération de police administrative. Dans le cadre d'une surveillance hiérarchique, l'individu doit être informé de ce possible suivi.

CONCLUSION DU TITRE II

460. **Les limites de la surveillance de l'internaute naviguant sur le web**. Le titre II a montré que le contrôle de l'identité de l'internaute connecté au réseau ne peut ressortir que de la mise en œuvre du pouvoir régalien. Ainsi les adresses IP circulant sur le réseau peuvent être librement collectées par les administrateurs de réseaux locaux ou par les sites web qui ne pourront obtenir la corrélation de celles-ci avec les coordonnées d'un abonné, et la localisation du point d'accès utilisé, que dans le cadre du déclenchement d'une action pénale. Par ailleurs les services de l'État sont fondés à surveiller les connexions au réseau en vue de la prévention de troubles à l'ordre public. Toutefois les conditions de la révélation de données permettant l'identification de l'internaute connecté sont soumises à un régime strict d'autorisation qui limite ces réquisitions administratives.

De plus il faut affirmer un principe général d'effacement des données révélant les choix de navigation de l'internaute qui peuvent à son insu l'identifier. Elles doivent être effacées au point d'accès au réseau par toute personne attribuant à la connexion une adresse IP valide. Au point d'arrivée de la communication, les moteurs de recherche et les navigateurs web ne peuvent par défaut enregistrer la navigation ; toute fonction d'historique devrait être soumise au consentement de l'internaute. Ainsi la visualisation des faits et gestes de l'internaute qui peut être légitime n'interviendrait qu'à rebours de cet effacement, suivant un régime d'interception au contenu précisé qui ne peut être que ponctuel et limité.

CONCLUSION DE LA SECONDE PARTIE

461. **Les principes à mettre en œuvre pour garantir les libertés d'accès et de naviguer de l'internaute**. Il n'est de liberté d'accès au réseau que si l'internaute y accède anonymement. L'internaute n'a pas à décliner son identité civile pour se connecter au réseau. Une telle politique ne peut ressortir que d'un État autoritaire.

Cela dit, cet anonymat n'est jamais total en ce que l'adresse IP attribuée le temps de la connexion permet de retrouver l'internaute connecté. L'adresse IP n'est pas l'identifiant d'un individu mais celui d'un point d'accès au réseau localisé physiquement. Un fichier doit être mis en œuvre par les pouvoirs publics pour organiser cette cartographie des points d'accès au regard des adresses IP attribuées aux connexions. Un tel fichier permet le contrôle de l'identité de l'internaute qui n'est jamais automatique mais procède d'une logique d'investigation pour considérer qui s'est connecté à partir de ce point.

Dès lors il n'est de liberté de naviguer sur le web que si l'internaute est assuré que sa navigation ne fait pas l'objet d'une surveillance arbitraire. Ainsi il ne peut être soumis à un contrôle d'identité que dans le cadre de poursuites pénales ou de procédures administratives strictement encadrées pour respecter les libertés qui lui sont constitutionnellement garanties. Par ailleurs il doit être affirmé que ses choix de connexion ne peuvent être connus, par principe, de personne. Par exception, une interception des données matérialisant sa navigation peut être mise en œuvre de manière ponctuelle mais elle doit répondre d'une finalité légitime, qui ne peut procéder que d'un pouvoir hiérarchique ou sécuritaire et qui doit être encadrée par un régime défini.

CONCLUSION GENERALE

462. **Les libertés de la personne physique sur ce nouvel espace qu'est internet.** La recherche d'une cohérence des intérêts à protéger sur le réseau a conduit à considérer la sauvegarde des libertés de l'individu sur le réseau, à l'instar de celle de ses libertés physiques. Au titre de ces libertés, sont protégées la liberté individuelle, entendue comme le fait de ne pouvoir être arbitrairement détenu, et la liberté d'aller et venir. Il doit en aller de même sur le réseau. Cette démarche invite à consacrer deux nouvelles libertés, propres à l'internet : la liberté d'accès au réseau et la liberté de naviguer sur le web.

463. **L'enjeu démocratique de la liberté d'accès au réseau**. Le ressenti du fort enjeu démocratique de l'accès au réseau fait apparaître que celui-ci devrait être garanti à tout citoyen. Toutefois cette exigence n'est affirmée dans aucun texte. A l'ère numérique, un mouvement tend à faire entendre la nécessité de nouveaux droits sur le réseau ; la volonté de constitutionnalisation d'un « droit à l'accès » apparaît de loin en loin dans l'actualité sans pourtant qu'elle se concrétise. En réalité, la formulation maladroite de « droit à » et les prétentions libertaires qui, à l'origine, étaient liées à cette revendication, paralysent cet effort de consécration d'un nouveau droit.

La méthode adoptée dans cette étude a été d'envisager l'accès au réseau non pas comme un nouveau « droit à » renvoyant à une créance subjective, qui peut paraître indéfinie, mais comme une nouvelle liberté publique, engageant l'État vis-à-vis des citoyens. La liberté d'accès au réseau est un principe, propre à une société démocratique et peut être formulée ainsi : « L'accès au réseau est libre ». Ce principe implique la mise en œuvre d'un service public de l'accès qui s'inscrit dans la limite de la satisfaction de l'intérêt général. Il se réalise aujourd'hui en France selon des mécanismes éprouvés.

Toutefois cette politique publique de l'accès au réseau n'est pas menée à son terme, alors que cette liberté n'est pas formellement consacrée par les textes. C'est ce à quoi cette thèse tente de remédier.

464. **La constitutionnalisation de la liberté d'accès au réseau**. Il est affirmé dans cette étude que la liberté d'accès au réseau doit être envisagée comme une liberté de premier rang. Elle conditionne toutes les autres. Elle est le pendant de la liberté individuelle du citoyen eu égard à la nouvelle capacité d'action que lui permettent le réseau et ses applications.

La liberté individuelle est entendue ici au sens strict que lui donne l'article 66 de la Constitution qui énonce que : « *Nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi*». Cette formulation fait ici écho à la sûreté, terme se trouvant à l'article 2 de la Déclaration des droits de l'homme et du citoyen, lequel a deux acceptions ; la sûreté renvoie tout à la fois à la garantie de la sécurité juridique, mais également à l'enjeu concret de la protection physique de l'individu qui ne peut être détenu de manière arbitraire. Comme il a pu être souligné : « *La volonté des rédacteurs de 1789 était également plus concrètement, de donner aux citoyens l'assurance qu'il n'y aurait plus de lettres de cachet et que l'expression, par exemple, de ses opinions ne le conduirait plus en prison »*[875]. Cet aspect de la sûreté est celui de *l'habeas corpus* britannique. Or cette approche sied parfaitement à la constitutionnalisation de la liberté d'accès au réseau : l'individu n'est libre d'agir sur le réseau et de mettre en ligne du contenu sur le web que dans la mesure où la privation de son accès fait l'objet d'un régime défini.

A la suite de l'article 66 de la Constitution, on pourrait envisager un article 66 bis ainsi rédigé : « *Nul ne peut être arbitrairement privé de son accès à un réseau de communications électroniques* ». Cette privation d'accès est possible, mais uniquement pour sanctionner des infractions limitativement énoncées par la loi. De plus, un second alinéa pourrait être également calqué sur celui de l'article 66 : « *L'autorité judiciaire est également gardienne de cette liberté* ». Le garant de la liberté d'accès au réseau est le juge judiciaire qui doit veiller à ce que cette sanction privative de liberté soit nécessaire et proportionnée au but poursuivi. Toutefois la compétence du juge judiciaire doit se limiter à cette mise en œuvre de la privation d'accès, alors que par ailleurs toute action sur les connexions, comme le blocage d'un site, ne s'apparente pas à une mesure privative de liberté. Le régime de la liberté de naviguer sur le web peut faire l'objet de restrictions qui peuvent être décidées par la puissance publique.

[875] FAVOREU L., *et al., Droit des libertés fondamentales*, 7ème éd., Paris : Dalloz (Précis, droit public, science politique), 2016., n°215-2.

465. **Le caractère spontané de la liberté de naviguer sur le web**. L'étude soutient dans un second temps que doit être affirmée la liberté de naviguer sur le web. Une analogie est établie avec la liberté d'aller et venir. Celle-ci est aujourd'hui rattachée par le Conseil constitutionnel à la liberté personnelle des articles 2 et 4 de la DDHC. Il y a donc autonomie de la liberté d'aller et venir laquelle ne relève pas de l'article 66 de la Constitution. La difficulté est qu'un degré de contrainte fort sur la liberté d'aller et venir d'un individu, sans toutefois que celui-ci soit emprisonné, peut s'apparenter à une mesure privative de liberté qui nécessite le contrôle du juge judicaire.

Toutefois, sur le réseau, ce débat entre mesure privative et restrictive de liberté est vite clos. Actuellement seuls des États, qui de fait sont autoritaires, agissent sur l'acheminement des connexions d'une manière telle que l'accès même au réseau de communication est vidé de son sens parce que l'individu n'a en réalité accès qu'à une sélection de sites et de services. En revanche, si cette contrainte mise en œuvre *ex nihilo* sur les connexions n'a pas lieu, il faut considérer que la liberté de naviguer sur le web se réalise spontanément une fois l'accès garanti. Toutefois, cette liberté de naviguer sur le web doit dans son intérêt même faire l'objet de restrictions de la part de la puissance publique à laquelle il appartient de veiller à la sauvegarde de l'ordre public sur le web. A cet endroit, l'étude souligne qu'il faut être vigilant alors que, par un raisonnement critiquable, il est affirmé que dès lors que le juge judiciaire en référé seulement, intervient s'agissant d'une mesure de blocage, les libertés de l'internaute sont sauves.

Il est soutenu que eu égard au respect de la liberté de navigation de tout internaute sur le réseau, la mesure de blocage d'un site ne peut être déclenchée par une initiative privée quand bien même cette mesure serait ordonnée par le juge judiciaire en référé. L'action du juge judiciaire n'est pas en tant que telle protectrice des libertés individuelles, elle l'est dans le cadre du contrôle d'une mesure prise par la puissance publique qui est seule investie d'un pouvoir lui permettant de limiter la liberté de tous. Ainsi une action en justice ne peut légitimer une mesure de blocage. Or il ne s'agit pas non plus de considérer que l'action de l'État à cet endroit doit être soumise au contrôle du juge judiciaire. Le blocage d'un site ou d'un service du web est une mesure restrictive de liberté qui peut répondre d'un régime de police administrative.

466. **Le régime de la liberté de naviguer sur le web**. S'agissant de la limitation des sites et services accessibles, seuls les pouvoirs publics ont vocation à intervenir dans le cadre d'un pouvoir de police qui toutefois ne peut être que spécial. En effet, il est vain de tenter de définir un ordre public numérique, alors que sur le réseau aucune circonstance particulière de

temps et de lieu ne peut venir matériellement limiter un pouvoir de police administratif général. Ainsi, le pouvoir administratif doit être habilité par le législateur à prendre une telle mesure qui procède de la règlementation d'une activité définie ou qui considère la protection de l'ordre public s'agissant d'un trouble spécialement défini.

Cette gouvernance des sites accessibles étant établie, les pouvoirs publics sont par ailleurs fondés à limiter l'accès de certains sites et services à des audiences spécifiées ou au contraire à interdire toute discrimination dans l'accès à certains sites. En revanche, la règlementation de la liberté de naviguer sur le web ne peut pas ressortir d'une pénalisation de la consultation habituelle de certains sites. Seule la consultation habituelle de sites à caractère pédopornographique peut être sanctionnée en tant que telle.

467. **Les principes à mettre en œuvre pour sauvegarder ces libertés.** La liberté d'accès au réseau et la liberté de naviguer sur le web, définies et garanties par un régime adéquat, n'ont de sens que si l'individu a accès au réseau anonymement et ne fait pas l'objet d'une surveillance arbitraire lorsqu'il navigue sur le web. L'étude soutient à cet endroit que la réflexion devant mener à considérer la mise en œuvre de tels principes ne relève pas de la protection des données personnelles. De plus, l'étude fait apparaître que le régime visant les données relatives au trafic met en œuvre ces objectifs de manière très imparfaite.

468. **Le respect de l'anonymat de l'internaute connecté au réseau**. L'individu n'est pas libre si l'ensemble de ses actions peuvent être ouvertement reliées à son identité civile.

Or la technique de l'adressage du réseau qui attribue un numéro unique à chaque connexion semble contrevenir à ce principe. Il est affirmé dans cette étude qu'il ne faut pas définir l'adresse IP comme une donnée à caractère personnel. Cette adresse peut être reliée à un individu identifié ; elle est traitée automatiquement, puisque produite nécessairement à chaque connexion ; mais elle ne permet pas l'identification immédiate de l'internaute par toute personne qui la détient. Il est ainsi proposé de la considérer comme le simple visage de l'internaute. Les traits d'un visage permettent d'identifier un individu, mais jamais automatiquement, et il faut s'en garder. L'identification procède uniquement d'une investigation qui nécessite la mise en œuvre de moyens humains. L'identification à partir de l'adresse IP relève de la même logique.

Le mécanisme d'adressage du réseau ne doit pas être dévoyé, en utilisant par exemple un procédé de masquage de l'adresse IP, mais inversement l'identité civile de

l'internaute ne doit pas être requise pour qu'il se connecte. En revanche, un fichage des points d'accès au réseau doit être mis en œuvre pour permettre cette identification.

469. **La définition d'une obligation générale de localisation des points d'accès au réseau.** A toute adresse IP circulant sur le réseau doit pouvoir être associée la localisation physique du point d'accès qui l'a émise pour considérer qui était présent physiquement à cet endroit au moment de la connexion. Or, actuellement, le régime de la conservation de certaines données relatives au trafic organise très maladroitement la mise en œuvre d'un tel fichier. Cette étude définit le contenu et le régime d'une obligation nouvelle de localisation des points d'accès au réseau. Toute personne qui attribue à un point d'accès une adresse IP doit être à même de répondre de cette action ; c'est-à-dire qu'au regard d'une adresse IP relevée sur le réseau, elle doit être capable d'y associer la localisation de l'accès au réseau qui matériellement l'a émise. Et, si besoin, une investigation permettra de remonter jusqu'à l'identification de l'individu.

470. **Les conditions du contrôle de l'identité de l'internaute**. L'individu qui navigue anonymement sur le web ne peut être soumis à une surveillance arbitraire. Les conditions du contrôle de son identité à partir de l'adresse IP attribuée à sa connexion doivent être définies.

Cette étude affirme un principe de liberté de collecte des adresses IP circulant sur le réseau. Cette collecte réalise l'interaction nécessaire qui doit intervenir entre l'internaute et le réseau local ou le site web auquel il se connecte. Cette collecte de données ne porte pas atteinte à la liberté de naviguer de l'internaute alors que la divulgation du point d'accès associé à l'adresse IP collectée ne peut résulter que d'une action pénale ou de l'exercice d'un pouvoir de police.

Dès lors, en revanche, il convient d'encadrer strictement toute opération de surveillance du réseau par les pouvoirs publics, laquelle consisterait en une collecte automatique des adresses IP se connectant à un site web spécifié en vue de prévenir des troubles à l'ordre public. Ce que fait de manière appropriée le nouveau cadre général visant toute opération de renseignement, défini dans le Code de la sécurité intérieure.

471. **Le principe d'effacement des données révélant la navigation de l'internaute**. La thèse soutient enfin, qu'un principe général d'effacement des données révélant les choix de navigation de l'internaute le temps de sa connexion doit être affirmé. Il est délimité alors qu'il ne vise que les données de navigation qui peuvent identifier l'internaute à son insu. Cependant il doit transcender les qualifications des différents acteurs du réseau.

Toute personne attribuant une adresse IP à la connexion d'un internaute ainsi que les interfaces permettant la navigation sur le web, que sont les logiciels navigateur et les sites de moteurs de recherche, doivent effacer les données révélant les sites web consultés et les informations recherchées.

Le suivi de la navigation d'un internaute ne peut ainsi être envisagé que dans le cadre d'un régime d'interception de telles données ; il ne peut procéder que d'un pouvoir sécuritaire ou hiérarchique. La mise en œuvre d'une telle filature numérique est ponctuelle et s'inscrit dans une durée limitée. Elle doit être autorisée par un juge dans le cadre d'une opération de police judiciaire ou répondre du régime strict d'une opération de renseignement. Dans le cadre de la mise à disposition d'un accès, les internautes doivent être informés de cette possible surveillance via la charte informatique.

472. **« Tout prévoir est impossible »**. En 1973, Adolphe Touffait, procureur général près la Cour de cassation, dans une tribune sur les libertés publiques et l'informatique, affirmait que : « *L'histoire de nos libertés publiques fait apparaître des appels passionnés à la liberté et de brutales restrictions, mais elle nous apprend qu'elles n'existent qu'en droit positif* »[876]. La complexité et la rapidité d'évolution des techniques ne doivent pas faire oublier cette affirmation de bon sens. Toute technique porte en elle ses futures avancées, mais il faut se garder de croire au mythe qu'elle puisse un jour déborder son créateur. « *Tout prévoir est impossible* »[877], être prescient l'est encore moins. Il convient d'être pragmatique et serein.

[876]TOUFFAIT Adolphe, « Libertés publiques et informatiques », Rapport présenté au Colloque de Pavie de la Société Internationale de Défense sociale, *Gaz. Pal.*, 9 août 1973, Doctrine, p.513.

[877] PORTALIS, *Discours préliminaire au premier projet de code civil,* an VIII.

Table des matières

Bibliographie

I. Dictionnaires

Vocabulaire juridique. CORNU G. (*dir.*), Association Henri Capitant, 12ème éd. Paris : P.U.F. (Quadrige), 2018

Dictionnaire de la culture juridique, ALLAND D. et S. RIALS (*dir.*), Paris : Lamy, P.U.F., (Quadrige-Dicos Poche) 2003

II. Cours, Manuels et Répertoire

BALLE F., *Médias et Sociétés,* 17ème éd., Paris : L.G.D.J Lextenso éditions, 2016

BIOY X., *Droits fondamentaux et libertés publiques*, 5ème éd., Paris : Montchrestien, Lextenso éditions, 2018 (LMD édition, Collection cours, *dir.* B. Beignier).

BONFILS P. et E. GALLARDO, « Secret des correspondances », *Rép. Dalloz Dr. Pén*

BOULOC B., *Pénologie,* 3ème éd., Paris : Dalloz, 2005 (Précis)

BURDEAU G., *Les libertés publiques,* 4ème éd., Paris : Librairie générale de droit et de jurisprudence, 1972.

CADIET L., JEULAND E., *Droit judiciaire privé,* 9ème éd., Paris : LexisNexis(Manuel), 2016

CARON Ch., *Droit d'auteur et droits voisins,* 5ème éd., LexisNexis Litec (Manuel) : Paris, 2017

CÉRÉ J.-P. « Prison (normes européennes) », *Rép. Dalloz Dr. Pén. et Proc.pén*.

CARBONNIER J., *Droit civil Introduction.* 27éd. refondue Paris : P.U.F, 2002, (Thémis Droit privé).

CASTETS-RENARD C., *Droit de l'internet,* 2ème éd., Paris : Montchrestien, Lextenso éditions(Cours, *coll.*, B. Beigner (*dir.*)), 2012

CORNU G., *Droit civil, Introduction au droit,* 13ème éd., Paris : Montchrestien, 2007 (Domat, droit privé)

DEBET A., MASSOT J., METALLINOS N., Informatique et Libertés, la protection des données personnelles en droit français et européen, L.G.D.J., Paris, 2015

DREYER E., *Droit pénal général,* 4ème éd., Paris : LexisNexis Litec (Manuel), 2016

FAVOREU L., *et al.*, *Droit des libertés fondamentales,* 7ème éd., Paris : Dalloz (Précis, droit public, science politique), 2016.

FRIER P. L. et J. PETIT
- *Droit administratif,* 12ème éd., Issy-les-Moulineaux : LGDJ Lextenso Editions, 2018
- *Précis de droit administratif,* 6ème éd., Paris : Montchretien, Lextenso éditions Domat, droit public), 2010

GAUTIER P.-Y., *Propriété littéraire et artistique,* 10ème éd., P.U.F (Coll. Droit fondamental classique) : Paris, 2017.

HOLLANDE A. et X. LINANT DE BELLEFONDS, Pratique du droit de l'informatique et de l'internet, 6ème éd., Paris : Edition Delmas, 2008

HUET J. et E. DREYER, *Droit de la communication numérique,* (Manuel), Paris : L.G.D.J. 2011

LUCAS A., DEVEZE J., FRAYSSINET J., *Droit de l'informatique et de l'Internet,* Paris : P.U.F. (Thémis Droit privé) 2001

MORANGE J.,
-*Les libertés publiques,* 8ème éd., Paris : P.U.F., 2007 (coll. QSJ)
-*Manuel des droits de l'homme et des libertés publiques,* Paris : P.U.F. Droit, 2007 (Manuels, Collection droit fondamental dirigée par Stéphane Rials)

OBERDORFF H., *Droits de l'homme et libertés fondamentales,* 6ème éd., Paris : L.G.D.J, Lextenso éditions, 2017 (manuel).

PRADEL J., *Droit pénal Général,* Editions Cujas, 21ème éd., Paris : 2016.

RIVERO J., MOUTOUH H., *Libertés publiques,* Tome I, 9ème éd., Paris : P.U.F. Droit (Thémis, droit public)

SCHMELCK R. et G. PICCA, *Pénologie et droit pénitentiaire,* Paris : Éditions Cujas, 1967

SUDRE F., *Droit européen et international des droits de l'homme,* 13ème. éd., Paris : P.U.F, 2016

TRUCHET D., Cours annuel, « Liberté d'expression, droit de la presse et de la communication audiovisuelle », Master 2 *Droit de la communication,* université Panthéon-Assa Paris 2, année 2006-2007

VEDEL G., DELVOLVE P., *Droit administratif,* 12ème éd., Paris : P.U.F. (Thémis Droit) 1992

WALINE J., *Droit administratif,* 27ème éd., Paris : Dalloz (Précis), 2018

III. Thèses et monographies

BATIFFOL H., Choix d'articles rassemblés par ses amis, PARIS : L.G.D.J., 1976

BERMAN P. S., *Law and society approaches to cyberspace.* 2007, Ashgate Publishing (The international library of essays in law and society),

CARBONNIER J.,
-*Flexible droit*, 10ème éd., Paris : L.G.D.J, 2014
-*Droit et passion du droit sous la Vème République,* Paris : Flammarion (Champs essais),1996

DELMAS-MARTY M. *Les forces imaginantes du droit (III),* Paris : Seuil (coll. La couleur des idées), 2007

DESGENS-PASANAU G., FREYSSINET E., *L'identité à l'ère numérique*, Paris : Dalloz, 2009 (Presaje)

FERAL-SCHUHL C., « Cyberdroit, le droit à l'épreuve de l'internet, 7ème éd., Paris : Dalloz *(*Praxis Dalloz), 2018

GALLOUEDEC F. GENUY S. et MAISL H., *Le secret des fichiers,* Institut français des sciences administratives, cahier n°13-1976, Paris : éditions Cujas, 1976

GENY F.,
- *Méthode d'interprétation et sources en droit privé positif : essai critique*, 2ème éd., Paris : LGDJ, 1919. (Publié une première fois en 1899).
-*Des droits sur les lettres missives, étudiés principalement en vue du système postal français,* Recueil Sirey : Paris, 1911.

GEORGEL J., *Les libertés de communication,* Paris : Dalloz (Connaissance du droit, droit public), 1996

FLAHERTY D. H. " Protecting privacy in surveillance societies, The Federal Republic of Germany, Sweden, France, Canada, and the United States" UNC Press Books, 1 févr. 1992

KAYSER P., *La protection de la vie privée par le droit, Protection du secret de la vie privée*, 3e éd., Paris : Économica, Aix-en-Provence (PUAM) 1995, 605pp

KUNER Ch.,
-*Transborder data flows and data privacy law*, Oxford University Press : 2013.
-*European Data Protection Law: Corporate Compliance and Regulation*, 2nd édition, Oxford University Press : 2007

LEPAGE A., Libertés et droits fondamentaux à l'épreuve de l'Internet, Paris : Litec, 2002

PICHARD M., *Le droit à, étude de législation française,* Paris : Economica, 2006 (Recherches juridiques)

QUEMENER M., FERRY J., *Cybercriminalité, défi mondial et réponses,* Paris : Economica, 1997

SOLOVE D. J.,

-*Nothing to Hide, The False Trade between Privacy and Security*, Yale University Press, 2011

-*The digital person, technology and privacy in the information age*, New-York University Press, 2004

IV. Mélanges et Ouvrages collectifs
(*par ordre chronologique)*

Mélanges offerts à Monsieur le professeur Pierre Voirin, Paris : LGDJ, 1966

Le secret et le droit, Travaux de l'Association Capitant, tome XXV, 1974

L'unité du droit, Mélanges en hommage à Roland Drago, Paris : Economica, 1996

Le droit du multimédia, de la télématique à Internet, HUET P. (*dir.*) Rapport de l'AFTEL : association française de la télématique et du multimédia, Paris : Les éditions du téléphone, 1996.

L'avenir du droit, Mélanges en l'honneur de François Terré, Paris : Dalloz, 1999

François Gény, mythe et réalités 1899-1999 centenaire de Méthode d'interprétation en droit privé positif, essai critique. THOMASSET C., VANDERLINDEN J et P. JESTAZ (*dir.),* Les éditions Yvon Blais, Dalloz, Bruylant Bruxelles, 2000 (thèmes et commentaires, études), 2000

The intensification of surveillance, Crime, terrorism and warfare in the information age, BALL K. and F. WEBSTER (*dir.),* London: Pluto Press, 2003.

Études offertes au Doyen Philippe Simler, Paris : Dalloz, Litec LexisNexis, 2006

La sécurité de l'individu numérisé, réflexions prospectives et internationales, S.LACOUR (*dir.*), Paris : L'Harmattan 2008

Lessons from identity trail, anonymity, privacy and identity in a networked society, edited by I.KERR, V.STEEEVES, and C.LUCOCK, Oxford University Press, 2009.

L'influence du droit européen sur les catégories de droit public, J.-B. AUBY (*dir.*), Paris : Dalloz (coll. Thèmes et commentaires), 2010

La communication numérique, un droit, des droits, B.TEYSSIE (*dir.*), Paris : Editions Panthéon-Assas, 2012

La pensée de François Gény, O.CACHARD, F-X LICARI, F. LORMANT (*dir*.) Paris : Dalloz, (Thèmes et commentaires, Actes), 2013

L'ordre public numérique, libertés, propriétés, identités, Ph. MOURON et C. PICCIO (*dir*.), Aix-en-Provence : PUAM (inter-normes coll.), 2015

V. Rapports et avis

NORA S., MINC A, *L'informatisation de la société, Rapport à M. le Président de la République* (remis le 20 janvier 1978), Paris : Seuil (coll. Points), 1978

IMBERT-QUARETTA M., *Outils opérationnels de prévention et de lutte contre la contrefaçon en ligne*, Rapport à Madame la ministre de la culture et de la communication, mai 2014

ROBERT M., *Protéger les internautes- Rapport sur la cybercriminalité*, Rapport aux ministres Christiane Taubira, Arnaud Montebourg et Bernard Cazeneuve et à la secrétaire d'Etat au Numérique Axelle Lemaire, groupe inter-ministériel de travail sur la lutte contre la cybercriminalité et présidé par le Procureur général Marc Robert, juin 2014

MENDEL T. et al, *Etude mondiale sur le respect de la vie privée sur Internet et liberté d'expression,* Paris : Editions Unesco (coll. Unesco sur la liberté de l'Internet), 2013

ARCEP
« L'accès à l'Internet, les entretiens de l'autorité, 18 janvier 2000 », document disponible sur le site de l'ARCEP, www. arcep.fr

CNIL
L'adresse est une donnée personnelle pour l'ensemble des CNIL européennes , Communiqué de la CNIL en date du 2 Août 2007, disponible sur le site de la CNIL.
La publicité ciblée en ligne, communication présentée en séance plénière le 5 février 2009, par B. Peyrat, rapporteur, disponible sur le site de la CNIL.

Conseil d'État
Le numérique et les droits fondamentaux, étude annuelle 2014, *Les Rapports du Conseil d'État* (ancienne collection Étude et documents du Conseil d'État), p.110, (édité par la Documentation française.

Internet et les réseaux numériques, étude adoptée par l'Assemblée générale du Conseil d'État le 2 juillet 1998, (Collection études du Conseil d'État)

Conseil national du numérique
Citoyens d'une société numérique, accès, littératie, médiations, pouvoir d'agir : pour une nouvelle politique d'inclusion, Rapport à la Ministre déléguée chargée des petites et moyennes entreprises de l'Innovation et de l'Économie numérique, Octobre 2013

Neutralité des plateformes : Réunir les conditions d'un environnement numérique ouvert et soutenable, Rapport à Arnaud MONTEBOURG, Ministre de l'Economie, du Redressement productif et du Numérique et à Axelle LEMAIRE, Secrétaire d'Etat chargée du numérique, juin 2014

Contrôleur général des lieux de privation de liberté
Avis du contrôleur général des lieux de privation de liberté (Jacques Delerue) du 20 juin 2011 relatif à l'accès informatique des personnes détenues, JORF du 12 juillet 2011, texte 82 sur 134.
Rapport d'activité 2013, Paris : Editions Dalloz, 2014.

Forum des droits sur l'internet
Recommandation du Forum des droits sur l'internet sur la « Publicité ciblée sur Internet » en date du 8 mars 2010

Groupe dit de « l'article 29 ».
-Avis 34/2000 sur le « Le respect de la vie privée sur internet- une approche européenne sur la protection des données en ligne», novembre 2000, WP 37
-Avis 4/2007 sur le concept de donnée à caractère personnel, adopté le 20 juin 2007, 01248/07/FR WP 136.
-Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, adopté le 4 avril 2008, 00737/FR WP 148

Rapport d'activité de la personnalité qualifiée prévue par l'article 6-1 de la loi n° 2004-575 du 21 juin 2004
« Rapport d'activité 2015 de la personnalité qualifiée prévue par l'article 6-1 de la loi n°2004-575 crée par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, mars 2015-février 2016 » M. Alexandre Linden

« *Rapport d'activité 2017 de la personnalité qualifiée prévue par l'article 6-1 de la loi n° 2004-575 du 21 juin 2004, crée par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, mars 2017-février 2018* » M. Alexandre Linden

VI. Articles

AUDIGOU A., « La protection pénale des télécommunications », *JurisPTT, la revue du droit des PTT,* n°6, octobre 1986

BALL K., WEBSTER F., "The intensification of surveillance"*, in "The intensification of surveillance, Crime, terrorism and warfare in the information age",* Ball Kirstie and Frank Webster (*dir.),* Pluto Press, 2003.

BATIFFOL H., «Droit comparé, droit international privé et théorie générale du droit », *in* Battifol Henri, *Choix d'articles rassemblés par ses amis,* PARIS : L.G.D.J., 1976

BEDARIDA F., « Histoire et pouvoir dans 1984 » in *Vingtième siècle, revue d'histoire*, n°1 janvier 1984, p.8.

BETTATI M., « Un statut international pour internet ?», p.97, *in La communication numérique, un droit, des droits*, B.TEYSSIE (*dir.*), Paris : Editions Panthéon-Assas, 2012

BEZZAZI E. H., « Identité numérique et anonymat : concepts et mise en œuvre », p.77, *in La sécurité de l'individu numérisé, réflexions prospectives et internationales*, S. LACOUR (*dir.*), Paris : L'Harmattan, 2008

BONAN F., « Violation du secret des correspondances par un particulier », *JurisPTT, la revue du droit des PTT*, n°15, 1er trimestre 1989

BOSCO D. « GAFA et droit de la concurrence », *CCC*, avril 2016, repère n°4

BURGORGUE-LARSEN L., « Libertés publique(s) et droit fondamental », p.286, *in L'influence du droit européen sur les catégories de droit public,* J.-B. AUBY (*dir.*), Paris : Dalloz (coll. Thèmes et commentaires), 2010

CACHARD O., L'obligation d'identification dans la loi du 1er Août 2000 (modifiant la loi du
30 septembre 1986 relative à la liberté de communication », article mis en ligne le 1er octobre 2000 sur le site du CEJEM.

CAPELLO A., « Retour sur la jurisprudence du Conseil constitutionnel relative aux sanctions administratives », *RSC* 2014, n°15

CAPRIOLI E., « Notification des violation de données à caractère personnel », *CCE* 2011, comm.116

CARAGLIANO D., « Real names and responsible speech : the cases of South Korea, Russia, and Facebook », working draft, *The Right to Information & Transparency in the Digital Age*, Stanford University, March 11-12, 2013.

CARDON D., « L'identité comme stratégie relationnelle », *Hermès La Revue*, n°53, 2009, p. 61

CHARRIER B., « Le consentement exprimé par les mineurs en ligne », *Dalloz IP/IT*, numéro 6-juin 2018

CEHAN A., « Sécurité, frontières et surveillance aux États-Unis après le 11 septembre 2001 », *in* « Surveillance politique, regards croisés », *Cultures et Conflits : sociologie politique de l'international,* Paris : L'Harmattan, août 2004, n°53

CHASSIGNEUX C. « Regards sur la violation de données à caractère personnel », *CCE* n°12, Décembre 2011, étude 23.

CHRESTIA Ph., « La loi du 23 janvier 2006 relative à la lutte contre le terrorisme, premières observations », *D.* 2006, p.1409

COHEN D., « Le droit à… », *in L'avenir du droit, Mélanges en l'honneur de François Terré*, Paris : Dalloz, 1999

COHEN J., « Examined lives : informational privacy and the subject as object", *Stanford Law Reviexw,* n°52, may 2000, 1373.

CORDIER G., « Focus sur la directive 2009/136/CE du 25 novembre 2009 modifiant la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques : optons pour une interprétation pragmatique des cookies », *RLDI,* n°57, février 2010, p. 1904.

CRIQUI G., « La fourniture d'une simple adresse IP est-elle suffisante ? Ou quand l'obligation à la charge de l'hébergeur doit être précisée. », *RLDI,* 05/2009, perspectives-analyse n°49.

DECOCQ A., « Rapport sur le secret de la vie privée en droit français », p.479, *in Le secret et le droit,* Travaux de l'Association Capitant, tome XXV, 1974

DE LAMY B., « Hadopi 1 : Précisions du Conseil constitutionnel sur le pouvoir de punir », *RSC.* 2010.209.

DEMPURE F., « Le classement des sites par les moteurs de recherche », *JCP G.*, n°10-11, 10 mars 2014, Tendances, p.326

DERIEUX E.,
- « Les principes du droit de la communication dans la jurisprudence du Conseil constitutionnel, de la liberté de communication au droit à la communication », *Légipresse*, n°141, mai 1997, II-50.
-« Liberté ou surveillance, fondements et éléments du droit de l'internet », *RLDI*-2011, études n°74.
- « Provocations et apologie du terrorisme », *Revue européenne des médias et du numérique*, n°33, hiver 2014-2015, p.5.

DIEU F.
-« Dissimulation du visage : la confirmation d'un interdiction de large portée-à propos des circulaires du 2 mars 2011 et du 31 mars 2011, *JCP adm.*, 2011, 2144
-« Le droit de dévisager et l'obligation d'être dévisagé : vers une moralisation de l'espace public ? », *JCP adm.* 2010, 2355

DREYER E.,
- « Le blocage de l'accès aux sites terroristes ou pédopornographiques », *JCP G*, n°14, 6 avril 2015, p.685.
-« Restaurer le contrôle des publications étrangères », *JCP G*, n°40, 4 oct. 2006, I 174.
-« La fonction des droits fondamentaux dans l'ordre juridique », *D. 2006*, n°11, p.748.

DROUARD E., BLANCHARD M., « L'adresse IP est-elle une donnée personnelle ? », *Légipresse*, n°255, octobre 2008, p.185.

EWALD François, « Le Triomphe de la notion de risque » extraits de *L'état-providence* (Paris : Grasset, 1986) *in Problèmes politiques et sociaux*, La Documentation Française, octobre 2007

FAVOREU L.,
- *Revue française de droit constitutionnel*, n°22, 1995, p.362.
-« Le droit constitutionnel jurisprudentiel en 1981-1982 », *RD publ.* 1986, p.387.

FRYDMAN B. « Le projet scientifique de François Gény », in *François Gény, mythe et réalités 1899-1999 centenaire de Méthode d'interprétation en droit privé positif, essai critique*. THOMASSET C., VANDERLINDEN J et P. JESTAZ (*dir.)*, Les éditions Yvon Blais, Dalloz, Bruylant Bruxelles,(thèmes et commentaires, études), 2000

GANDY O. H., "Data Mining and surveillance in the post 9/11 environment" in *The intensification of surveillance, Crime terrorism and Warfare in the information age,* K.BALL & F. WEBSTER (*dir.*), Pluto Press 2004

GAUBIAC Y., « Logiciels de distribution de musique peer-to-peer. Affaire RIAA c/ Verizon », *CCE*, mars 2004.

GAUTIER P.-Y., «Réflexions sur François Gény, l'actualité méthodologique de *Science et technique », in La pensée de François Gény,* O.CACHARD, F-X LICARI, F. LORMANT (*dir*.) Paris : Dalloz (Thèmes et commentaires, Actes), 2013

GINOCCHI D., « Le contrôle de la LOPPSI par le Conseil constitutionnel », *AJDA* 2011, p.1097.

GORCHS B., «Vers un référé de l'Internet autonome », *CCE* 2007, étude 31.

HUET P., « Les services multimédias » *in Le droit du multimédia, de la télématique à Internet,* HUET P. (*dir.),* (Rapport de l'AFTEL : association française de la télématique et du multimédia), Paris : Les éditions du téléphone, 1996

HUSTINX P. « Protection des données à caractère personnel en ligne : la question des adresses IP », *Légicom,* n°42-2009-1, p.125

IMBERT-QUARETTA M. et al, « La contravention de négligence caractérisée à la lumière de la mise en œuvre de la procédure de réponse graduée », *JCP G*, n°19, 7 mai 2012, étude n°591.

KAYSER P., « Le principe du secret des lettres confidentielles et ses rapports avec le principe de droit public de la liberté et de l'inviolabilité de la correspondance », p.437-465,
in Mélanges Pierre Voirin, Paris : LGDJ, 1966

LASSERRE-CAPDEVILLE J., « Les problèmes liés à l'adresse IP en matière bancaire *Dalloz IP/IT,* 219, avril 2017

LAUGEE F.
- « L'ARCEP, gendarme de la neutralité de l'internet », *REM* n°28, automne 2013, p.14.
-« Neutralité du Net : les opérateurs télécoms américains gagnent leur bataille », *Revue Européenne des Médias (REM),* n°29 hiver 2013-2014, p.53.

LAZERGUES C., « La lutte contre le terrorisme peut-elle mettre en danger la liberté d'expression ? », *Légipresse,* n°321, novembre 2014, p.579.

LECLERQ P., « Un d'application de la législation" informatique et libertés " », Chronique « un an de … », *CCE*, octobre 2007

LEMIEUX T. « La responsabilité de l'abonné internet en cas de contrefaçon en ligne, regard français sur l'affaire *BearShare* », *RLDI,* 2014/109, p. 17-22,3600.

LORRAIN A.-C., MATHIAS G., « Données de connexion : la publication du premier décret ou la première pierre d'un édifice encore inachevé », *RLDI*, n °17, juin 2006, p.37.

LEVADE A., « Epilogue d'un débat juridique : l'interdiction de la dissimulation du visage dans l'espace public validée », *JCP G* 2010, 1043

LEROYER A.M., « La circulaire et le voile : interrogations sur une notion émergente : « Les exigences minimales de la vie en société », *RTD civ.*, 2011, p.399

MBONGO P., Préface, *in L'ordre public numérique, libertés, propriétés, identités,* Ph. MOURON et C. PICCIO (*dir.*), Aix-en-Provence : PUAM (inter-normes coll.), 2015

MACREZ F. et GOSSA J., « Surveillance et sécurisation : ce que l'Hadopi rate, à propos de la « petite loi » « Création et Internet » », *RLDI* 2009/50, n°1659, p.80.

MAISL H., « La protection des données et des systèmes » *in Le droit du multimédia, de la télématique à Internet*, HUET P. (*dir.*), (Rapport de l'AFTEL : association française de la télématique et du multimédia) Paris : Les éditions du téléphone, 1996

MALLET-POUJOL N., « Droit des communications électroniques (Mars 2017-Mars 2018) », *Légipresse*, avril 2018.

MANARA C., « La « search neutrality » : mythe ou réalité ? », *Concurrences*, N°1-2011, Doctrines, p.53.

MARINO L., « Le droit d'accès à Internet, nouveau droit fondamental », *D.*2009 n°30, Point de vue, p.2045.

MASTOR W., « La loi sur le renseignement du 24 juillet 2015 : « La France, Etat de surveillance ? », *AJDA* 2015, p. 2018

MILLAR J., "Core privacy: a problem for predictive data mining" in *Lessons from identity trail, anonymity, privacy and identity in a networked society,* edited by I.KERR, V.STEEEVES, and C.LUCOCK, Oxford University Press, 2009

MORANGE J., « La crise de la notion de liberté publique » *in L'unité du droit, Mélanges en hommage à Roland Drago*, Paris : Economica, 1996, p.91.

NOSSOVITCH M.-C., « Les utilisations délictuelles du kiosque télématique », *JurisPTT, la revue du droit des PTT*, n°25, 1990.

ODILON-BARROT, « Du privilège des imprimeurs et de leurs obligations envers le public », *Annales de législation et de jurisprudence,* / [Th. Compans, rédacteur principal], n°1 samedi 16 mai 1829, p.5 (Disponible sur Gallica.fr).

OCQUETEAU F., « La « sécurité globale », une réponse à la menace terroriste ? », *in* « L'État face aux risques », *Regards sur l'actualité,* Paris : La documentation Française, février 2007

POLLAUD-DULLIAND F., Chronique de propriété littéraire et artistique, *RTD. Com,* avril/juin 2008, p. 302.

ROLIN F., SLAMA S., « Les libertés dans l'entonnoir de la législation anti-terroriste », *AJDA,* 2006 p.975.

SCHMIDT-SZALEWSKI J., « L'internet ou l'illusion libertaire *», in Mélanges Simler,* Paris : Dalloz, Litec LexisNexis, 2006

SEGUR P., « Le terrorisme et les libertés sur l'internet », *AJDA* 2015, p. 160.

SIMON Ch., « Les adresses IP sont des données personnelles selon le Conseil constitutionnel », *RLDI,* juillet 2009, n°51, 1701.

SZUSKIN L., GUILLENCHMIDT (de) M., «La qualification de l'adresse IP au centre de la lutte contre le téléchargement illicite sur les réseaux peer-to-peer *», RLDI,* déc. 2007, n°1095 ;

TEYSSIE B., « L'homme et la fourmi, variations sur l'empire du numérique », p.55, *in La communication numérique, un droit, des droits,* B.TEYSSIE (*dir.*), Paris : Editions Panthéon-Assas, 2012

TOUFFAIT A., « Libertés publiques et informatiques », Rapport présenté au Colloque de Pavie de la Société Internationale de Défense sociale, *Gaz. Pal.,* 9 août 1973, Doctrine, p.513.

VERPEAUX M. « Dissimulation du visage, la délicate conciliation entre la liberté et un nouvel ordre public », *AJDA* 2010, 2373

VILA J.B. « L'ouverture à la concurrence des jeux d'argent et de hasard en ligne : "première étape ou simple palier" d'une régulation ? », *AJDA* 2010 p.1366.

WACHSMANN P., « De la marginalisation du juge judiciaire en matière de libertés et des moyens d'y remédier », *D.* 3mars 2016, n°9, éditorial.

WU T., « Network Neutrality, Broadband Discrimination», *Journal of Telecommunications and High technology law,* 2003, vol. 2, p.143

ZOLYNSKI C., ROCHFELD J., « La "loyauté" des "plateformes". Quelles plateformes ? Quelle loyauté ? » *Dalloz IP/IT*, nov. 2016, p.523.

VI. Notes de jurisprudence et commentaires de décisions

BERNAUD V., GAY L, SEVERINO C., Décision n°2005-532 DC du 19 janvier 2006, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers « Droit constitutionnel », *D.* 2007, p.1166

BOUBEKEUR I., CA Paris, 14ème ch. sect.B., arrêt du 4 février 2005, *S.A. BNP PARIBAS c/ Société WORLD PRESS ONLINE*, « Une entreprise peut se voir attribuer la qualité de fournisseur d'accès à l'Internet », article mis en ligne le 04 avril 2005, sur le site juriscom.net

BRUGUIERE J.-M., Décision n° 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur internet*, « Loi "sur la protection de la création sur internet" : mais à quoi joue le Conseil constitutionnel ? », *D.* 2009, n°26, point de vue, p.1771.

DEBET A.,
- Cass., com., 18 juin 2013, n°12-28488, « Refus de transmission de QPC par les jeux en ligne par la Cour de cassation », *CCE* 2013, *comm*. 114.
- CEDH, 18 déc. 2012, n°3111/10, *Ahmet Yildrim c/ Turquie*, « Blocage de "Google site" : la Cour européenne des droits de l'homme condamne la Turquie », *CCE*, juillet 2013, comm.77.

CARON C.,
-TGI St-Brieuc, 6 septembre 2007, nº 05003922, Ministère public et SCPP c/ M. J. P, Juris-data : 2007/349373 « Qualification de l'adresse « IP » : état des lieux jurisprudentiels », *CCE*, 2007 n°12, comm. 144.
-CJCE (aff. C-275/06), 29 janvier 2008, *Promusicae c/ Telefonica de Espana SAU*., « La communication de données personnelles dans le cadre d'une procédure civile à l'aune du droit communautaire », *CCE*, mars 2008, commentaires n°32, p. 25.
- Cass. 1ère civ. 19 juin 2008, n°07-12244, *CCE* 2008, *comm*.99
- Cass. crim., 13 janvier 2009, n°08-84088, *Bull. crim.* 2009, n°13, « Validité des constats effectués par des agents assermentés »,*CCE.*, avril 2009, n°31, p.25
- CJUE, 27 mars 2014, aff. C-314/12 *UPC Telekabel Wien c/ Constantin Film Verleih Gmbh* « Le blocage de sites contrefaisants une nouvelle fois devant la Cour de justice de l'Union européenne », *CCE*, 2014, comm. 43

CASTETS-RENARD C., CJUE 8 avr. 2014, Digital Rights Ireland c/Ireland C293/12 et C594/12, *D.* 2014, n°23, note. p.1355

CHAUVIN E., Cass. crim., 20 mai 2015, n°14-81336, *Bull.crim.* 2015, n°119, « Hacker n'est pas jouer, maintien et vol de données dans un système automatisé de traitement de données », *LPA*, 29 juillet 2015, n°150, p.15.

COUSSIRAT-COUSTERE V., CEDH 24 avr. 1990, Huvig et Kruslin c/ France, Série A, nos 176-A et 176-B, *Annuaire Français de Droit International (AFDI)*, 1991. 606, obs.

CRIQUI G., Cass. Soc. 9 juillet 2008, n° 06-45800, *Bull.*, 2008, V., n°150, « " les connexions établies par un salarié sont présumées avoir un caractère professionnel"» Arrêt de la chambre sociale de la Cour de Cassation du 9 juillet 2008 », article initialement mis en ligne le 4 décembre 2008 sur le site du CEJEM.

DALEAU J., CJCE (aff. C-275/06), 29 janvier 2008, *Promusicae c/ Telefonica de Espana SAU.*, « Droit d'auteur et protection des données à caractère personnel : arrêt rendu par la Cour de justice des Communautés européennes, gde.ch, 29 janvier 2008, n°C-275-06 », *D.*,2008, p.480.

DECOCQ G.
-Décision du Conseil de la concurrence n°00-D-31 du 9 juin 2000 relative à une saisine au fond et une demande de mesures conservatoires présentées par la société Concurrence (BOCC, 25 juill. 2000, p.422), « Première rencontre entre le droit de la concurrence et les pratiques en matière de nommage et de recherche de site », *CCE* 2000, n°11, comm., n°119
- CA de Paris le 25 novembre 2015, « Google n'a pas eu de stratégie d'éviction sur le marché de la cartographie », *CCC*, janvier 2016, comm. n°19.

DERIEUX E.,
- CJCE (aff. C-275/06), 29 janvier 2008, *Promusicae c/ Telefonica de Espana SAU*., « Le droit communautaire n'impose pas que les législations nationales prévoient l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile », *JCP G.*, 2008, n°21, II. 10099.
-Cass. crim., 13 janvier 2009, n°08-84088, *Bull. crim.* 2009, n°13, « Lutte contre la contrefaçon et protection des données personnelles », *Légipresse*, n°261, mai 2009, p.98.

EL SAYEGH D., Décision n° 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur internet*, « Le Conseil constitutionnel et la loi Création et Internet : une décision en trompe l'œil », *Légipresse*, n°263 Juillet/Août 2009, tribune p.97.

FLAMENT L.,
- Cass. crim., 13 janvier 2009, n°08-84088, *Bull. crim.* 2009, n°13, « Les constatations visuelles effectuées sur internet, sans recourir à un traitement préalable de surveillance automatisé ne constituent pas un traitement de données à caractère personnel (à propos de l'arrêt de la chambre criminelle du 13 janvier 2009) », *Dr. Pén.*, mai 2009, études 10, p.11
-« Le numéro d'IP n'est pas une donnée à caractère personnel-La cour d'appel de Paris persiste et signe ! », *Dr. Pén.*, n°12, décembre 2008, étude 27.

FROMENT (de) B., (commissaire du gouvernement), CE, 6 février 1991, *Burki*, Req.n°49663, *AJDA*, 20 juin 1991, jurisprudence p.467.

GRYNBAUM L., TGI Paris, 3ème ch. réf., 4 déc. 2014, *affaire dite « The Pirate Bay »*, *RLDI* 2015, actu112.

HOQUET-BERG S., Cass. 1ère. Civ.,19 juin 2008, n°07-12244, *Bull.*, 2008, I, n°178. « Pouvoirs du juge des référés à l'égard des fournisseurs d'accès à l'internet », *Resp. civ. Assur.*, 2008, comm. 256.

HUGON C., Cass. 1ère civ. 19 juin 2008, n°07-12244, *Bull.* 2008, I n°178, *JCP G* 2008, n°42 II 10171.

LASSERRE-CAPDEVILLE J., TGI Metz, 8 Décembre 2010, *L'essentiel du Droit Bancaire,* fév. 2011, *obs.*, p. 6.

LE GOFFIC C., CA Paris, pôle 5, chambre 1, arrêt du 15 mars 2016, « Décision Allostreaming : légalité des mesures de déréférencement et coût de blocage à la charge des intermédiaires techniques », *Dalloz IP/IT* 2016, 372.

LEPAGE A., Décision n°2005-532 DC du 19 janvier 2006, Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers « Censure partielle de la loi relative à la lutte contre le terrorisme », *CCE,* mai 2006, n°86, p.43.

LE POITTEVIN, Cass. Crim., 5 novembre 1903, *DP* 1904 I. 25, note

LESUEUR J., CJCE (aff. C-275/06), 29 janvier 2008, *Promusicae c/ Telefonica de Espana SAU*. V., « La balance sans l'épée : la droit fondamental sans l'effectivité », *Légipresse,*n°250, avril 2008, p. 57

LOISEAU G., Cass. com, 10 déc. 2013, n°12-28488, *CCE* 2014, comm. 17.

MAILLARD S., Cass. Soc. 17 juin 2009, n°08-40274, *Bull.* 2009, V., n°153, *Sté Sanofi Chimie c/M. Guzzi et al*, « L'administrateur réseau peut ouvrir les messages personnels des salariés dans le cadre de sa mission », *JCP G,* n°39, 21 sept. 2009, n°263, p.22.

MALAURIE-VIGNAL M., CA Paris, pôle 1, ch. 2, 28 mai 2015, *Contrats Concurrence Consommation,* 2015, *comm.* 227

MANARA C.,
- CJUE (aff. C-70-10), 25 novembre 2011, *Scarlet Extended SA c/SABAM et al*, *D.* 2011, 2925, obs.
-Décision du Conseil de la concurrence n°00-D-32 du 9 juin 2000 relative à une saisine au fond et une demande de mesures conservatoires présentées par la société Concurrence (BOCC, 25 juill. 2000, p.422), « Exercice d'une activité de commerce électronique : accession au domaine « .fr » et ententes », *D.* 2000, AJ, p. 391.

METALLINOS N., CA Montpellier, 3ème ch., 22 mars 2017, n°15-17729 *M.X. c/Overblog,* « Vers une garantie du pseudonymat sur les forums de discussion ? », *CCE,* mai 2017, n°48, p.32.

NADEAU A., ROQUEFEUIL (de) B, CA Rennes, 3ème ch. Corr., 22 mai 2008, RG n°07/01495, C.S. c/Sacem ; CA Rennes 3ème ch. Corr, 23 juin 2008, T.L. c/SCPP ; CA Rennes, 3ème ch. Corr ,11 décembre 2008, *Gaz. Pal, 23/24 janvier 2009,* note p.40

PERONNE G., DAOUD E., Cass., civ. 1ère., 3 nov. 2016, 15-22595, FS+P+B+I *Cabinet Peterson c/ groupe Logisneuf et autres.* « L'adresse IP est bien une donnée à caractère personnel », *D. IP/IT,* 120, février 2017.

PIGNATARI O.,
-CA Paris, pôle 5, chambre 1, arrêt du 15 mars 2016, *APC et al c/ Auchan télécom et al.*, *RLDI* 2013/99, n°3293.
-TGI Paris, réf. 28 nov. 2013, *APC et al c/ Auchan télécom et al.*, « Blocage et déréférencement de plusieurs sites de streaming : à qui profite le stream ? », *RLDI* 2013/99, n°3293.

PRADEL J., CEDH 24 avr. 1990, Huvig et Kruslin c/ France, Série A, n^{os} 176-A et 176-B, *D.*1990. 353, note

RIBES D., Décision 2000-441 DC du 28 décembre 2000, loi de finance rectificative pour l'année 2000. *D.* 2001, somm. P. 1842, obs.

ROBERT J.H., Cass. crim., 13 janvier 2009, n°08-84088, *Bull. crim.* 2009, n°13 : « Le travail manuel de l'informaticien », *Dr. Pén.*, mai 2009, commentaires 66, p.30

SCHOETTL J.E.-, note sous Conseil constitutionnel n°2005-532 DC (Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers), *Gaz. Pal.*, 7 février 2006, n°38, p.20.

STOFFEL-MUCNK Ph., Cass. 1ère civ., 19 juin 2008, n°07-12244, *Bull.* 2008, I n°178, *CCE* 2005, comm. 140.

SZUSKIN L., DE GUILLENCHMIDT M, CJCE (aff. C-275/06) *Promusicae c/ Téléfonica de Espana Sau*, « L'arrêt « Promusicae » : beaucoup de bruit pour rien ? », *RLDI*, avril 2008, actualités, n°37.

TELLER M., Cass. crim., 13 janvier 2009, n°08-84088, *Bull. crim.* 2009, n°13, « Les difficultés de l'identité numérique : quelle qualification juridique pour l'adresse IP ? », *D.*2009, n°29, chronique p.1988

VERPEAUX M., Décision n° 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur internet*, « La liberté de communication avant tout, la censure de la loi Hadopi 1par le Conseil constitutionnel », *JCP*, 2009, n°39 du 21 septembre, étude 274, p.49

VÉROT C. (commissaire du gouvernement), CE, 23 mai 2007, n°288149, *SACEM et al.*, Juris-Data n°2007-071900, *AJDA*, 16 juillet 2007, p. 1413

Commentaires aux Cahiers du Conseil constitutionnel
Commentaires aux Cahiers, Décision n°2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI),disponible en ligne sur le site du Conseil constitutionnel,* www.conseil-constitutionnel.fr

Commentaire de la décision n°2009-580 DC -10 juin 2009, Loi relative à la diffusion et à la protection de la création sur internet, 2009-580 DC, *Les cahiers du Conseil constitutionnel*, n°27, 2009, p. 101.

VIII. Autres

BARDEAU F., DANET N., *Lire écrire compter coder*, Editions FYP (France), 2014

BATELLE J., *La révolution Google,* Paris : Eyrolles, 2006

BORRADORI G., *Le « concept » du 11 septembre, dialogue à New-York (oct. Déc. 2001), avec Giovanna Borradori, Jacques Derrida, Jürgen Habermas,* Paris : Galilée, 2004.

ECO U., *Le nom de la Rose,* Paris : Grasset, 1982

FOUCAULT M., *Surveiller et Punir, naissance de la prison,* Paris : Gallimard (*tel),* 1975, (impression 20 janvier 2007, p. 234).

FANTI S., *Alcatraz Numérique,* Vevey, Suisse : éd. Xénia, 2009,

FRANCQ P., *Internet, Tome 1 : La construction d'un mythe,* Bruxelles : E.M.E (Editions Modulaires Européennes) (Techno, logos, ƐƮ Polis), 2011

GOLDSMITH J., T.WU, Who Controls the Internet, Illusions of a Borderless World, Oxford University Press, 2006

LOWE D., *Créer son réseau pour les nuls*, Paris: Editions First, 2010.

MARTEL F., *Smart, enquête sur les internets,* Paris : Stock, 2014.

MONTESQUIEU, *De l'esprit des lois,* (tome I), Paris : Garnier-Flammarion, 1979

ORWELL G., *1984,* Paris : Gallimard, 1950 (*folio,* janvier 2008)

PIAZZA P., *Histoire de la carte nationale d'identité,* Paris :Odile Jacob (Odile Jacob histoire), 2004

PILLOU J-F., Tout sur les réseaux, 3ème éd., Paris : DUNOD, (Commentçamarche.net), 2012

SOULEZ S. *Le Marketing,* Paris : Gualino Extenso editions (coll. Les Zoom's), 2008

VIRIEUX F., *Comment marche Internet ?,* Paris : Editions le Pommier, (Les petites pommes du savoir), 2004

TANZER N., *Philosophie politique,* Paris : P.U.F., 1994

ZWEIG S., *Le Monde d'hier souvenirs d'un européen*, Bermann-Fisher Verkag AB Stockholm, 1944 (Belfond, Le Livre de Poche, Editions 1er coffret, novembre 2011).

IX. Allocutions et Conférences

CARDON D., allocution du sociologue, lors du colloque organisé par le M2 Droit du multimédia et de l'Informatique de l'Université de Paris 2, « Les réseaux sociaux, quels enjeux juridiques », le 6 mars 2009.

LECLERCQ P., allocution du Conseiller à la Cour de cassation lors que colloque « Banque et Internet », organisé par le CEJEM, le jeudi 11 juin 2008

LOUVEL B., 1er président de la Cour de cassation, « L'autorité judiciaire, gardienne de la liberté individuelle ou des libertés individuelles ? Réflexion à l'occasion de la rencontre annuelle des premiers présidents de cour d'appel et de la Cour de cassation », allocution du 3 février 2016, disponible sur le site de la Cour de cassation, www. courdecassation.fr

MAIGRON P, ingénieur à l'institut Télécom/TélécomSudParis, « La racine du DNS : bien commun ou fragmentation », intervention lors du colloque du CEJEM-Université Panthéon-Assas, « Les philosophie de l'Internet : conciliation possible avec le droit, » du 9 juin 2011.

SERRES M., « *Les nouvelles technologies, que nous apportent-elles ?* », conférence de Michel Serres, enregistrée à l'École Polytechnique le 1er décembre 2005, faisant partie du cycle *Culture Web*, coordonné par Serge Abiteboul, dans le cadre des Thématiques INRIA. Disponible au format mp3 sur le site : interstices.info, rubrique « débattre ».

SCOTTIEZ F., intervention intitulée « L'adresse IP, une donnée à caractère personnel ? ». lors de la conférence « L'adresse IP : une empreinte digitale sur internet ? » organisée par le Master 2 Droit du multimédia et de l'Informatique et le CEJEM (Centre d'études juridiques et économiques du multimédia) de l'université Paris 2, jeudi 2 mars 2017.

THOUMYRE L., intervention lors du Colloque « Les réseaux sociaux, quels enjeux juridiques ? », du 6 mars 2009 organisé par le master 2 « Droit du multimédia et de l'informatique », de l'université de Paris 2.

X. Articles de presse et mis en ligne sur le web

Presse française

BARRE N., « Contrôler Internet ? », éditorial du journal *Les Echos* du lundi 23 juin 2008.

BOUCHER Ph., « Safari ou la chasse aux français », *Le Monde,* le 21 mars 1974

COMBIER E., « Fin de le neutralité du Net aux Etats-Unis », article mis en ligne le 11 juin 2018, sur le site des *Echos*, www.lesechos.fr

GIRARDEAU A., « L'Europe étourdit Hadopi », article mis en ligne le 7 mai 2009 sur le site du journal Libération, rubrique « médias », www.libération.fr

GRONDIN A., « Netflix mise sur la recommandation », *20minutes*, mardi *1*6 septembre 2014, p.15.

GIRARD L., « L'exploitation des informations privées à des fins commerciales aiguise les appétits », *Le Monde,* du vendredi 28 mai 2010, p.17.

HUSSON G., « Le Minitel, "faux-frère" d'Internet, ferme définitivement », article mis en ligne le 29 juin 2012 sur le site www.*LeMonde.fr*

LELOUP D., « La pénalisation des de la consultation de sites « terroristes », une proposition peu réaliste », article mis en ligne, le 22 mars 2012, sur le site *LeMonde.fr*

LELOUP D. et L.CHECOLA, « L'anonymat proscrit des réseaux sociaux à Pékin », article mis en ligne le 16 mars 2012 sur le site *LeMonde.fr*

LEPLÂTRE S., « En Chine, la reconnaissance faciale envahit le quotidien », *Le Monde,* lundi 11 décembre 2017.

MANENTI B., « Apologie du terrorisme : une longue liste de condamnations », article mis en ligne le 20 janvier 2015, sur le site www.nouvelobs.com

ORY-LAVOLLEE, « Création et Internet, inutile précaution ? », *Le Monde,* mardi 14 avril 2009.

SOULLIER L., « Dans le grand fourre-tout de l'apologie du terrorisme », article mise en ligne le 21 décembre 2015, sur le site *lemonde.fr.*

SUPLY L., « Les nouvelles trouvailles de la cyber-censure », article mis en ligne 2 janvier 2008 sur le site www.*Lefigaro.Fr*.

VIOSSAT S., « Menaces sur l'Internet libre et ouvert », *Les Dossiers de la Recherche (DLR)* #10-Juin/Juillet 2014, p. 22.

« Un détenu placé en garde-à-vue après s'être filmé un joint à la main sur Periscope », article mis en ligne le 22février 2016, sur le site *LeMonde.fr*

« La Corée revient sur un dispositif requérant l'identification des internautes », article mis en ligne le 27 Août 2012 sur le site *LeMonde.fr.*

« Les eurodéputés favorables à l'enregistrement des recherches web », », article mis en ligne le 21 juin 2010, sur le site *LeMonde.fr.*

« La poste : hausse inédite du prix du timbre au 1ER janvier 2015 », article mis en ligne le 1 octobre 2014 sur le site 20minutes.fr

Presse étrangère

BALL J, ARTHURAND C., GABATT A., « FBI claims largest Bitcoins Seizure after arrest of Silk Road founder", article mis en ligne le 2 octobre 2013 sur le site de *The Guardian,* *www*.theguardian.com

BARBARO M. et T. ZELLER, « A face is exposed for AOL searcher n°4417749 », *The New York Times*, édition du 9 août 2006.

EUNJUNG CHA A. « Le partage des données nous sauvera-t-il ? », article publié initialement dans le *Washington Post* et repris dans le *Courrier international* n°1130 du 28 juin au 4 juillet 2012, p.40

KANG C., " F.C.C. repeals net neutrality rules", article mis en ligne le 14 décembre 2017, sur le site du *NewYorkTimes*, www.nytimes.com.

LUHN A., "Russia offers 3.9m roubles for ´research to identify users of TOR´", article mis en ligne le 25 juillet 2014 sur le site *The Guardian*,

RAWLINS A., « How Philadelphia's prisons are embracing technology », article mis en ligne le 28 octobre 2014, sur le site de la chaîne d'information américaine CNN, www.cnn.com

ROSS C., « Reshma Saujani's ambitious plan for Technology », article mis en ligne le 5 novembre 2014, sur le site du *Wall Street Journal*, http://www.wsj.com.

D. WAKABAYASHI, A. SATARIANO, « How Facebook and Google could benefit from the G.D.P.R, Europe's New Privacy Law », article mis en ligne le 23 avril 2018sur le site *du New York Times*, *nytimes.com*

« Sorting out the Net », article mis en ligne le 24 Août 2012 sur le site du quotidien *koreajoongangdaily.joins.com.*

Sites spécialisés

HINAULT R., "Le W3C crée un groupe de travail pour la protection anti-traçage/ Google et Opéra continue de tourner le dos à Do not Track », article mis en ligne le 12 septembre 2011 sur le site developpez.com,

BERGE F., « *E-administration : 75% des français veulent plus de démarches en ligne* », article mis en ligne le 24/01/2014 sur le site www.01net.com

BERNE X. « En Californie, les délinquants sexuels obligés de se dévoiler sur le Net », article mis en ligne le 6 novembre 2012 sur le site www.*nextinpact.com*

CHAMPEAU G. « La Loi contre l'anonymat suspendue par la justice californienne », article mis en ligne le 7 novembre 2012 sur le site www.*numerama.com*

DELFAU V., « Google ramène la durée de conservation des données utilisateurs à 18 mois », article mis en ligne le 13 juin 2007, sur le site www.lemondeinformatique.fr.

GIRARDEAU A., « Conservation des données par les moteurs de recherche, l'Europe s'agite », article mis en ligne le 16 juin 2010 sur le site www.owni.fr

GUILLEMIN C., « L'arme de surveillance contre les utilisateurs de Napster » publié le 5 avril 2001, sur le site www.Zdnet.fr

JARVINEN H., "Russia and Austria take action against the use of TOR", article mis en ligne le 30 juillet 2014 sur le site de l'association EDRI (European Digital Rights), www.edri.org

LECLERCQ B., « La prison déconnectée », article mis en ligne le 1er mai 2012, sur le site www.Owni.fr

LUCKMAN E., « *Perludem gives developers access to big data about Indonesia's election",* article mis en ligne le 11 mars 2014, sur le site www.TechinAsia.com.

REES M., « FFT : les "net-goinfres" devront payer pour croquer plus » article mis en ligne le 22/08/2011 sur le site www.Nextimpaxt.com

SANYAS N.,
- « Orange dément préparer des "offres de débits différenciés"», article mis en ligne le 11/10/2012 sur le site www.Nextimpaxt.com
-« Combien de pages web y-a-t-il sur internet ? », article mis en ligne le 15 septembre 2011 sur le site : **www.pcinpact.com**

« Anti-tracking : Mozilla dévoile sa solution pour Firefox », article mis en ligne le 24 janvier 2011 sur le site generation-nt.com.

« Why Facebook just launched its own 'Dark web' site », article mis en ligne le 3 novembre 2014, sur le site du mensuel américain *Wired*, *www.wired.com*

« YouTube ne veut pas demander la carte d'identité de ses utilisateurs », article publié le 14 avril 2009 sur le site www.numerama.com

Blogs
« *Le monde du Minitel se paye Le Monde* », billet mis en ligne le 20 juin 2010 sur le blog « A l'œil » de Michel Puech, http://blogs.mediapart.fr/blog/michel-puech.

XI. Sites web

Dictionnaires et encyclopédies

www.cnrtl.fr

www.larousse.fr

www.linguee.fr

www.wikipédia.fr

www.wikipédia.org

Références

www.légifrance.gouv.fr.

www.eur-lex.europa.eu

www.legalis.net

www.ladocumentationfrancaise.fr/

www.mcj.fr

Sites institutionnels

- français

www.assemblee-nationale.fr

www.sénat-fr

www.conseil-constitutionnel.fr

www.courdecassation.fr

www.cnil.fr

www.arcep.fr

www.cglpl.fr

www.data.gouv.fr

www.culturecommunication.gouv.fr

www.etalab.gouv.fr

www.ecolenumerique.education.gouv.fr/.

www.economie.gouv.fr/france-numerique-2020/france-numerique-2020-0

www.cnnumerique.fr

www.culture.fr/franceterme

www.internet-signalement.gouv.fr

- Européens

www.ec.europa.eu/commission/index_fr

http://www.europarl.europa.eu/portal/fr

http://uis.unesco.org/

- Etrangers

www.garanteprivacy.it

www.justice.gov

www.iana.org

Autres

http://www-public.it-sudparis.eu/~maigron/Internet/

www.commentçamarche.net

www.futura-sciences.net

www.thenetmonitor.org

www.google.com/loon/

www.torproject.org

www.eff.org

Index

(Les chiffres renvoient aux numéros de paragraphes,

Les numéros en gras désignent les occurrences principales)

A

B

C

D

I

J

L

M

N

O

S

T

U

V

W

Résumé :
Cette étude envisage le réseau internet comme un nouvel espace invitant à réinterpréter les libertés de la personne physique. Au titre de celles-ci, sont protégées la liberté individuelle, entendue comme le fait de ne pouvoir être arbitrairement détenu et la liberté d'aller et venir. Il doit en aller de même sur le réseau. Etablissant une analogie avec ces libertés, la première partie de la thèse consacre deux libertés : la liberté d'accès au réseau et la liberté de naviguer sur le web. La première implique de définir le contenu d'un service public de l'accès. De plus, il faut affirmer que la coupure d'accès au réseau doit être envisagée comme une mesure privative de liberté ; elle ne peut donc être décidée que par le juge judiciaire. L'affirmation de la liberté de naviguer sur le web conduit à envisager le régime du blocage des sites, une mesure qui ne peut intervenir que dans le cadre d'une police administrative spéciale. Dans la seconde partie il apparaît que ces deux libertés n'ont toutefois de sens que si l'individu a accès au réseau anonymement et n'est pas surveillé arbitrairement quand il navigue sur le web. Cette étude cherche ainsi à préciser le régime devant encadrer le mécanisme d'adressage du réseau. Sont définies les conditions du contrôle de l'identité de l'internaute à partir de son adresse IP. Enfin, il est soutenu qu'un principe général d'effacement des données révélant les sites visités doit être affirmé, principe qui s'applique aux différents acteurs du réseau, notamment les moteurs de recherche. L'interception de ces données ne peut procéder que d'un pouvoir sécuritaire ou hiérarchique sur l'internaute.

Descripteurs :
Libertés publiques – Internet- Numérique- Communications électroniques- Accès au réseau- Anonymat sur le réseau- Adresse IP- Données personnelles- Surveillance- Informatique et libertés.

Title and Abstract: The protection of Individuals rights on the internet
This study considers the internet as a new territory where rights guaranteed to each individual in physical space can be promoted; not only free speech and privacy, but also the *Habeas Corpus* prerogative writ, which protects against unlawful imprisonment, and the right to freedom of movement. Thus, processing by analogy, the dissertation intends to promote two specific digital rights: the freedom to connect to the internet and the freedom to surf on the web. The freedom to connect should be part of a public service which promotes this access through public policies. Moreover, barring someone from using the internet can only be decided by a judge. The freedom to surf should protect the web users against unreasonable restrictions. Thus, measures blocking illegal websites should not come through self-regulation but through a legal framework which defines how administrative authorities are entitled to decide such restrictions. The protection of these two rights entails further obligations. Individuals must access the internet anonymously and they must be aware of how the government monitors their actions on the web. This study tries to outline the content of measures aiming to frame network addressing mechanisms. Identity checks based on the IP address should be subject to a strict legal regime. The study concludes that individuals have to be protected from surveillance when data reveal their choices among websites while they are connected. Internet access providers, but also search engines and browsers, must delete this data. Only special measures taken by a public entity or someone entitled to control the web users may lead to this kind of data retention.

Keywords:
Individuals rights-Digital rights- Internet- Electronic communications- Freedom to connect-Anonymity on the Internet-IP address-Surveillance -Data protection