

TABLE DES MATIÈRES

INTRODUCTION.....p.4

Titre I L'ordre public comme moyen d'orientation d'un ordre juridique global...p.10

Chapitre 1 Les raisons d'une sécurisation au travers de l'ordre public.....p.10

Section 1 L'État et l'obligation d'assurer la sécurité...p.11

Section 2 Risques et dangers du cyberspace.....p.14

Chapitre 2 Vers une sécurisation nécessaire de cet espace.....p.17

Section 1 La politique française de sécurisation et l'émergence d'une nouvelle régulation normative.....p.17

Section 2 Les outils de cette sécurisation.....p.20

Titre II La conciliation entre l'ordre public et liberté.....p.25

Chapitre 1 Une protection issue d'un large dispositif juridique.....p.25

Section 1 Notions et risques d'atteintes à la vie privée.....p.25

Section 2 Quelle protection pour les données personnelles ?.....p.28

Chapitre 2 L'impact d'un ordre public malléable.....p.31

Section 1 Vers un ordre public culturel ?.....p.32

Section 2 Pour une conciliation des différents intérêts p.36

BIBLIOGRAPHIE.....p.38

SITES INTERNET.....p.40

INTRODUCTION

« L'ordre, et l'ordre seul, fait la liberté. Le désordre fait la servitude. Seul est légitime l'ordre de la liberté. »¹

Cette célèbre phrase illustre encore et toujours l'éternel problème de la confrontation entre les droits et les devoirs de chaque citoyen vivant dans une démocratie.

Chaque liberté est encadrée dans la mesure où la vie sociale existe, ce qui exclut donc l'existence de libertés sans frontières.

De ce fait, afin de maintenir un ordre social, l'État apparaît comme le détenteur « du monopole de la violence physique légitime »².

La demande de sécurité de la part des citoyens est un fondement qui s'illustre bien à travers le fameux contrat social.

Et la conception de ce dernier par Thomas Hobbes illustre bien cette logique sécuritaire, qui du fait de l'anarchie qui peut exister et de « guerre de tous contre tous », oblige chacun à aliéner sa liberté et plus précisément les libertés individuelles, afin de vivre en sécurité.

Voilà comment s'illustre le rôle majeur de l'État qui doit veiller à la sécurité de ses sujets.

Cette stabilité issue de la perte d'une partie de liberté s'explique par le fait que la sécurité régule nos vies quotidiennes, tant au regard de notre intégrité physique que la protection de nos biens. Mais elle s'illustre aussi par exemple par la nécessité concernant la sécurité des moyens de transports.

Ainsi l'impact de cette exigence de sécurité dans notre vie, s'accroît sans aucun doute à travers l'essor des nouvelles technologies.

Or il est indéniable de constater une certaine ambivalence.

En effet, on remarque de la part des citoyens une exigence concernant leurs sécurités et la crainte que peut susciter sa mise en œuvre.

Car l'effet « big brother »³ agit rapidement lors de l'apparition ou de la révélation concernant un fichier informatique venant en aide aux forces de police, ou bien lors de projets de mise en place de systèmes de vidéosurveillance des espaces publics.

À noter sur ce sujet d'ailleurs un aspect de la loi LOPSI 2 (Loi d'orientation et de programmation pour la performance de la sécurité intérieure) en préparation qui risque de faire débat, réside dans le fait que la loi compte déléguer à des sociétés privées le visionnage des images enregistrées sur la voie publique. Ce qui peut présenter quelques risques notamment au regard de l'utilisation de ces images à des fins privées.

¹ : Charles Péguy, *Les Cahiers de la quinzaine*, bimensuel créé par ce dernier.

² : Max Weber, *Le savant et le politique*, Paris : Plon, 1959, 232 p.

³ : Georges Orwell, *1984*, Paris : Gallimard, 1972, 438 p.

Alors se pose le problème paradoxal de savoir quelle exigence de sécurité voulons-nous.

Sachant que celle-ci est forcément liée aux avancées technologiques, nous nous effrayons (et parfois à juste titre) de devoir accepter certaines contraintes et/ou des limitations à notre sentiment de liberté qu'offrent les outils technologiques permettant cette sécurité.

Ainsi comment garantir cette dernière au travers d'une législation qui ne soit pas, ou qui ne devienne pas liberticide.

Les nouvelles technologies permettent une prise de conscience qui semble être une évidence. Mais l'est-elle forcément ?

Car le citoyen doit saisir les enjeux de cette question qui affecte sa vie privée et pas seulement en tant que cyberconsommateur victime d'une fraude sur le cyberspace (« espace de communication créé par l'interconnexion mondiale des ordinateurs ; espace, milieu dans lequel naviguent les internautes »⁴) et réclamant une sécurité pour effectuer ses achats.

Cette sécurité englobe des enjeux qui vont au-delà de ces simples préoccupations, et qui affecte notre intimité au plus profond de nous-mêmes.

Cette cybercriminalité [« Ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet. On distingue les infractions liées aux technologies (virus, piratage, etc.), celles liées aux contenus (racisme, pédophilie, etc.) et celles facilitées par les réseaux (copie illicite de logiciels ou d'œuvres audiovisuelles, etc.).⁵] affecte aussi les entreprises qui sont parfois victimes de vols de données et selon une enquête menée par le Club de la sécurité de l'information français (CLUSIF) 75% des entreprises françaises ne mesurent pas régulièrement leur niveau de sécurité⁶.

Les citoyens exigent une sécurité qui ne soit pas trop contraignante accompagnée d'une qualité de protection concernant les éventuelles limitations de certaines libertés.

Comment concilier cette exigence de sécurité sans tomber dans un angélisme mièvre, et renonçant à certaines libertés, sans pour autant basculer dans une paranoïa irréaliste ?

La notion de liberté personnelle n'est pas définie juridiquement et ne fait pas l'objet d'une définition univoque, mais on connaît des notions similaires comme les libertés fondamentales, les libertés publiques, les libertés individuelles ou collectives.

Mais aucune de ces notions n'englobe réellement une conception propre au cyberspace comme pourrait l'être celle de liberté personnelle.

Elle pourrait se définir comme un ensemble de libertés qui comprendrait des droits comme le droit à la sécurité du cyberspace, le droit

⁴ : *Le nouveau Petit Robert de la langue française 2008*, Paris : Dictionnaires Le Robert, 2007, 2837 p., p.605

⁵ : *Le Petit Larousse illustré 2009*, Paris : Larousse, 2008, 1889 p., p. 278

⁶ : *Direct matin*, 436, 24 mars 2009, p.11

au respect de la vie privée, la liberté d'expression, et dans une certaine mesure, un droit à la sûreté.

Ce dernier peut être limité ou aménagé comme l'ensemble des droits et libertés dans un État de droit. Mais au regard de la problématique que représentent Internet et le monde virtuel, il faut concevoir ce droit comme le droit à la sûreté tel qu'il est évoqué aux articles 2, 7, 8 et 9 de la Déclaration des Droits de l'Homme de 1789, qui consiste à ne pas être arrêté, accusé ou détenu arbitrairement, ni d'être exposé à des peines qui ne seraient strictement pas nécessaires.

Or on constate que ce principe n'est pas en accord quant aux risques de certains utilisateurs du Réseau, relatifs à leurs engagements ou opinions.

Outre que ce dernier est cadencé dans certains pays, dans d'autres les législations s'adaptent au regard des risques pour la sécurité des États, mais aussi au regard d'intérêts bien différents.

Mais cette relative définition de cette notion de liberté personnelle s'adapte à notre approche du cyberspace. Ce dernier désigne un ensemble de données numérisées constituant un univers d'information et un milieu de communication, « lié à l'interconnexion mondiale des ordinateurs »⁷.

En effet, cette liberté personnelle illustre bien l'aspect individualiste du « moi » face au monde virtuel, mais aussi du « moi » face à ce monde réel.

Cette liberté reflète notre liberté de pensée, de conscience et d'opinion, au travers de nos agissements dans le cyberspace.

L'aspect formidable et le sentiment de liberté qu'offre le cyberspace permettent la pensée collective, la créativité, la prise de parole, voire la mobilisation, qui s'illustrent par exemple par le développement des blogs (« site Internet animé par un individu ou une communauté qui s'exprime régulièrement dans un journal, des billets »⁸), des forums (« espace virtuel consacré à l'échange de messages écrits, aux discussions sur un thème, en temps différé entre utilisateurs d'un réseau télématique »⁹) de discussion.

Cette « liberté personnelle » constitue le fondement de l'autonomie de la personne.

Alors se pose le problème du contrôle de cette autonomie par l'État sur le cyberspace.

Du moins sans pour autant parler d'un contrôle *stricto sensu*, mais plutôt d'un encadrement, en fonction de l'État où nous nous trouvons.

La liberté n'est pas la même si on se trouve en Chine où le cyberspace est verrouillé, aux États-Unis où il est très contrôlé ou en Europe.

Il est évident que cet espace doit être encadré afin d'éviter l'anarchie et à terme contribuer à sa destruction.

Ce problème est similaire à la gestion par un État de son territoire.

Ainsi toutes les libertés sont limitées et justifiées par la notion d'ordre public.

⁷ : *Le nouveau Petit Robert de la langue française 2008*, Paris : Dictionnaires Le Robert, 2007, 2837 p., p.605

⁸ : *idem* p. 266

⁹ : *idem* p.1082

On peut définir l'ordre public comme « un moyen d'assurer la protection ou la constitution de l'ordre social et juridique auquel il se rattache, en jouant les rôles d'exception, de réserve, de dérogation qui permettent, dans cette ordre juridique, de s'opposer à l'effet normal d'un principe, d'une norme, d'un droit, d'une liberté, pour la sauvegarde ou pour la promotion d'une valeur supérieure »¹⁰.

Cette notion constitue un des fondements du droit administratif, car il pose le principe de l'action de la police administrative, qui en tant qu'activité de service public a pour objet de prévenir toute atteinte à cet ordre et d'y mettre fin à travers des prescriptions règlementaires.

Dans un sens large il correspond à l'ensemble des exigences fondamentales considérées comme essentielles au fonctionnement des services publics, au maintien de la sécurité ou de la moralité.

À l'origine définie dans l'ancien article L131-2 du code des communes par la célèbre trilogie de tranquillité, sécurité et salubrité publiques, on constate que cette notion englobe de nombreux domaines.

Mais l'ordre public correspond « à un certain minimum de conditions essentielles à une vie sociale convenable dans une période donnée »¹¹.

Il est intéressant de noter que cette notion est à la fois relative et circonstancielle, elle tient compte d'éléments de temps et de lieux.

En effet, l'ordre public peut être national ou local, c'est-à-dire qu'il s'impose sur tout le territoire ou sur certaines de ces parties.

Mais il joue également à la fois un rôle directeur et protecteur.

On constate que si les finalités intrinsèques de l'ordre public sont plutôt intangibles, les exigences qu'elles impliquent aujourd'hui sont plus diverses et tendent à épouser les nouvelles conceptions du fonctionnement d'une société.

La définition de l'ordre public a évolué avec le temps.

Au début, il se fondait plus sur l'absence de troubles matériels.

Mais grâce à cet aspect changeant et malléable, l'ordre public permet la considération de nombreuses et de nouvelles préoccupations.

Ainsi il a permis de dégager de nouveaux principes inspirés comme par exemple de la Haute juridiction administrative avec la décision du 27 octobre 1995 « Commune de Morsang-Sur-Orge » concernant la dignité de la personne humaine ; ou celle du Conseil Constitutionnel relative aux lois sur la bioéthique (décision n°94-343-344 du 27 juillet 1994).

Cela permet, comme le souligne le Professeur Picard, que son contenu soit « virtuellement inépuisable et donc insaisissable ».

Il convient de remarquer qu'une notion qui est marquée d'une certaine imprécision ne permet pas de délimiter un contenu précis et exact.

Cependant ce caractère extensif de l'ordre public ne révèle pas une inexactitude et contribue à une harmonisation de l'ordre juridique global malgré son évolution.

Cette dernière s'est accentuée avec l'impact du droit communautaire. On remarque que les circonstances qui peuvent justifier le recours à l'ordre public peut varier d'un État à un autre : arrêt de la Cour de Justice des

¹⁰ : Étienne Picard, *La notion de police administrative*, Paris : Librairie générale de droit et de jurisprudence, 1984, 926 p.

¹¹ : Georges Vedel, *Droit administratif*, Paris : Presses universitaires de France, 1982, 174 p.

Communautés européennes 4 Décembre 1974 Yvonne Van Duyn c/Home Office 5 « les circonstances spécifiques qui pourraient justifier d'avoir recours à la notion d'ordre public, peuvent varier d'un pays à l'autre et d'une époque à l'autre.... ».

Dans le cadre de cette étude, nous nous attacherons plus à développer l'aspect sécurité, et on constate que ce dernier est souvent la cause invoquée dans l'utilisation de l'ordre public, qui a été proclamée « droit fondamental » conditionnant « l'exercice des libertés individuelles et collectives »¹².

À noter que le Conseil Constitutionnel a fait de la sécurité « un objectif de valeur constitutionnelle »¹³.

Il est vrai que la notion d'ordre public peut effrayer dans la mesure où il est l'outil permettant de restreindre certaines libertés.

Mais alors que penser si cette notion est qualifiée de sécuritaire ?

Le terme sécuritaire « tend à privilégier les problèmes de sécurité publique »¹⁴.

Alors l'encadrement de cet espace se justifie au regard des risques liés au cyberterrorisme, la pédopornographie, ou la cyberdélinquance qui posent de réels problèmes de sécurité publique.

On constate que la législation a évolué en tenant souvent compte de la notion d'ordre public, cependant cette évolution n'est pas propre au cyberspace ou propre au droit de l'Internet.

Il existe certes un ensemble de lois qui encadrent ce domaine mais pas un « corpus » bien distinct qui tient compte de la notion d'ordre public et du cyberspace.

Cependant l'aspect sécurité lié au cyberspace justifie certaines évolutions législatives prenant un aspect sécuritaire.

Dans quelle mesure cet espace doit-il être encadré ?

La sécurité est-elle le seul fondement à l'augmentation de lois diminuant notre liberté personnelle ?

Cela pose tout simplement « l'éternel problème de la conciliation du droit de l'individu avec le droit de la société, de la conciliation de l'ordre avec la liberté »¹⁵.

Au regard de certaines lois en vigueur, des sentiments divergents apparaissent et amènent à réfléchir sur la pénalisation de certains comportements.

On remarque que lorsqu'il règne un climat d'insécurité matérielle, la sensibilité et la crédulité sont exacerbées.

On peut donc craindre une justification d'éventuelles atteintes à des libertés du fait de la peur exprimée par les citoyens, en générant « *un capital d'inquiétude* »¹⁶.

¹² : Article 1° de la loi du 18 mars 2003 sur la sécurité intérieure.

¹³ : Décisions du 18 janvier 1993 et du 13 mars 2003.

¹⁴ : *ob.cit.* p.6, p.2339

¹⁵ : François Luchaire, *Naissance d'une constitution, 1848*, Paris : Fayard, 1998, 274 p., p. 55

¹⁶ : Didier Bigo, « Sécurité et immigration : vers une gouvernamentalité par l'inquiétude ? », *Cultures & Conflits*, 31-32, 1998, p. 13-38.

Cette dernière ne constitue pas le fondement même de l'utilisation de l'Internet ou du moins comme l'imaginaient ses créateurs.

Il convient d'apporter une précision concernant la définition d'Internet.

Il se caractérise de manière technique comme le réseau public mondial utilisant le protocole de communication Internet Protocol ou IP.

Il permet l'accès au public à des services comme le courrier électronique et le World Wide Web.

Ce dernier fait souvent l'objet d'une confusion avec Internet.

Cependant le Web ne constitue qu'une application d'Internet, comme peut l'être l'utilisation du courrier électronique.

Alors sous prétexte de sécurité, comment être sûr que nos agissements, nos opinions, ou tout un mode de vie ne soient plus l'expression de notre liberté mais le fruit d'un comportement que nous devrions adopter sous peine d'enfreindre la loi.

Cela a pour conséquence de modifier les rapports entre les États désireux de contrôler cette espace, et les citoyens voulant l'utiliser comme un espace de liberté affranchi d'un encadrement, déjà existant.

De nombreuses préoccupations apparaissent comme par exemple les questions concernant l'utilisation et la protection des données personnelles. Sachant que normalement toute donnée est prenable, sauf dans le cas de l'utilisation d'un système de cryptologie efficace.

Mais celui-ci est-il réellement libre ?

Ainsi au regard de ces nombreuses constatations et interrogations, il convient d'étudier cette apparente coexistence organisée, cet équilibre entre l'ordre public, et les libertés personnelles.

« En droit, l'impératif de sécurité doit servir d'instrument à l'exercice de la liberté. Il ne peut que la limiter que pour la servir »¹⁷.

La difficulté posée par ce sujet réside dans le fait que de nombreux points abordés peuvent faire l'objet d'études approfondies comme le cyberterrorisme, la protection des données personnelles, les questions de propriété intellectuelle, ainsi que de nombreux points non évoqués dans cette étude.

Cela s'explique par l'immensité des problématiques qui existent quant aux problèmes posés par le cyberspace.

L'axe de réflexion se porte plus sur la question de la sécurité, dans une première partie, nécessité qui s'applique au regard des risques pouvant affecter les États mais aussi les personnes privées, dans un contexte de globalisation de l'utilisation du cyberspace.

Ces risques qui augmentent de manière exponentielle, du fait de l'amélioration des technologies d'information et de communication, représentent un danger certain pour la vie privée et les données personnelles.

¹⁷ : Droit à la sécurité et libertés publiques. Jamil Sayah, *Les États face à la sécurité*, P.U.G., 2003, p. 387 et suivantes

Une problématique majeure se détache au regard de ces questions qui place au centre des préoccupations la confiance et le développement des usages de l'informatique.

Cet encadrement nécessaire, doit se faire dans un certain degré de proportionnalité, qui a des répercussions qui dépassent le simple cadre de la sécurité.

En effet, il est intéressant d'étudier l'impact de cet ordre public sur des aspects qui sont normalement moins contraignants au regard des libertés personnelles.

Cette ouverture sur le côté culturel avec la loi favorisant la création et la protection de la création sur Internet (HADOPI), pose de nombreux problèmes, et suscite autant d'interrogations, comme par exemple, dans le fait que les fournisseurs d'accès à Internet devront collaborer dans le suivi de leurs utilisateurs récalcitrants concernant le téléchargement.

Il paraît évident que des mesures doivent être prises dans certains cas, mais bien au-delà du problème du téléchargement, cette nouvelle forme de contrôle amène à une réduction de la liberté de chacun dans l'utilisation du cyberspace.

Ainsi l'enjeu majeur de la gestion du cyberspace réside dans la confiance entre les différents acteurs et les mesures nécessaires à sa régulation.

Titre I L'ordre public comme moyen d'orientation d'un ordre juridique global

Chapitre 1 Les raisons d'une sécurisation au travers de l'ordre public

Faut-il concevoir cet espace comme devant être uniquement sous le contrôle de l'État ?

Dans une certaine mesure, si nous reprenons le concept basé sur le fameux triptyque sécurité, salubrité, tranquillité publique, il est certain que l'État doit assurer sa propre sécurité, ainsi que celle de ses citoyens, y compris dans le monde virtuel, au vu des risques liés à ce dernier.

Section 1 L'État et l'obligation d'assurer la sécurité

Il existe plusieurs hypothèses où la sécurité de l'État peut être mise en péril par des attaques liées au cyberspace.

Ces attaques peuvent être le fait d'un État, ce qui jusqu'à présent est assez rare, soit le fait d'individus ou de groupes d'individus.

Aussi il faut concevoir de nouveaux types de conflits, et donc réfléchir aux mesures ou aux contre-mesures qui peuvent et qui doivent être adoptées, en fonction de leur probabilité.

Il faut tenir compte que tous les États de nos jours sont dépendants de l'informatique et des nouvelles technologies.

On peut se demander quel serait l'impact d'une attaque de grande envergure qui paralyserait tous les systèmes d'information et de communication d'un État comme la France provoquant ainsi une sorte de « *Pearl Harbor* » informatique. Ce scénario n'est pas le fruit d'une grande production cinématographique américaine, mais d'une possibilité bien réelle grâce à l'avancée des nouvelles technologies.

Car les attentats du 11 septembre ont modifié considérablement la conception de la sécurité d'un État.

Ce qui était impensable voire improbable pour les services de sécurité, l'est désormais aujourd'hui.

Ainsi de nombreuses lois sécuritaires sont apparues, comme le Patriot Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*) aux États-Unis, adopté par le Congrès le 26 octobre 2001, à la suite des attentats du 11 septembre 2001.

En France, les lois concernant la sécurité se sont multipliées comme la LCEN, la LOPSI et LOPSI 2 qui est actuellement en préparation.

À noter que la Convention européenne des droits de l'homme justifie certaines restrictions à certaines libertés, comme le précise l'article 8§2 : « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique, à la défense de l'ordre et à la prévention des infractions pénales... ».

Les risques liés au terrorisme sont réels et donc certaines mesures sont concevables.

Mais doit-on craindre des attaques terroristes de type cybernétique (« science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication dans l'être vivant et la machine.¹⁸ ») ?

Ce terme se définit comme la science des analogies maîtrisées entre organismes et machines.

Il a été formalisé par Norbert Wiener en 1947 qui considérait cette science comme permettant l'étude de manière exclusive des communications et leurs régulations dans les systèmes matériels et artificiels¹⁹.

On peut se demander si une attaque cyberterroriste est possible et donc à prendre au sérieux.

Il paraît peu probable ou du moins de douter de l'efficacité d'une attaque terroriste à une banque de données par Internet.

¹⁸ : *Ob.cit.* p.6, p.605

¹⁹ : Norbert Wiener, *Cybernetics, or Control and communication in the animal and the machine*, Paris: Hermann, 1948, 195 p.

Cependant la nocivité pourrait être bien réelle. Pour cela il suffit juste d'imaginer le chaos provoqué dans le cas d'un cyber sabotage.

Ainsi il peut être envisagé la paralysie d'un État et de ses services ministériels, du réseau de transports (comme pour le contrôle aérien), des services bancaires.

Cependant, comme l'énonce François-Bernard Huyghe, l'utilisation des outils technologiques par les partisans de la « guerre Sainte » est envisagée par le lien qu'il existe entre l'image et l'action.

En effet, la doctrine Jihadiste se fonde sur une politique de terreur qui s'amplifie grâce au pouvoir de l'image.

Ainsi les nouvelles technologies, et plus précisément Internet, sont plus utilisés pour des revendications, et donc constituent un moyen permettant de véhiculer une propagande.

Ces outils servent ainsi à la guerre de l'information voire de la désinformation.

De même, on peut douter de l'utilité du cyberspace pour les terroristes afin d' enrôler des kamikazes. Celui-ci sert plus pour transférer des informations par des boîtes mails de type Gmail ou Yahoo.

Alors ce cyberspace doit être surveillé sans pour autant remettre en cause la vie privée de chacun.

L'État a-t-il le droit de déroger à certains principes sous prétexte d'assurer sa sécurité.

Il paraît normal de tracer certains internautes qui peuvent présenter un risque pour la Nation du fait de leurs intérêts pour des sites comme « Aneada.com » ou « Azzan.com ».

Ces sites sensibles font l'objet d'une surveillance justifiée, mais il est certain que les cyberterroristes n'échangent pas d'informations pouvant compromettre leur organisation, et planifient encore moins leurs attaques sur ces sites.

Ce qui peut paraître logique au vu des moyens dont disposent les services de renseignements américains comme la NSA, qui utilisent des logiciels de cryptologie ou de déchiffrement pour filtrer les messages qui circulent par le Net.

Sans pour autant douter de la fiabilité de ces systèmes, on constate que la lutte contre le terrorisme ne peut se passer de l'aspect humain du renseignement.

Il convient d'envisager un autre type d'attaque cybernétique, comme par exemple le cas d'une guerre informatique entre États.

En avril 2007, l'Estonie a fait l'objet de plusieurs attaques informatiques qui ont notamment visé le Parlement, ainsi que certains ministères. Mais aussi des institutions privées comme les banques ou différents médias de communications.

Ces attaques provenaient de l'étranger et de forts soupçons se sont portés vers la Russie, sans pour autant pouvoir l'affirmer avec certitude²⁰.

Cependant, selon le Ministre estonien de la Défense de l'époque Jaak Aavisko, ces attaques faisaient suite à une décision visant à déplacer un monument de l'ère soviétique²¹.

Cet exemple illustre sans doute un des premiers cas d'attaque ou de guerre informatique d'un État envers un autre État.

Cette nouvelle technologie bouleverse la conception des conflits qui pourront surgir entre États et qui pourrait consister à « utiliser tous les moyens possibles, avec et sans la force des armes, avec et sans la puissance militaire, avec et sans victimes, pour obliger l'ennemi à satisfaire son intérêt propre »²².

²⁰ : Sujet ayant fait l'objet du documentaire intitulé « Cyber-guérilla » diffusé sur France 5 le mardi 10 mars 2009 à 20h55.

²¹ : Jaak Aavisko, *Real Threats From The Imaginary World, Vital Speeches of the Day*, janvier 2008, p.28

²² : Qiao Liang et Wang Xiangsui, *La Guerre hors limites*, Paris : Rivages, 2003

Il est utile de préciser que les attaques des sites gouvernementaux sont fréquentes. Ainsi on peut citer l'exemple des différents qui existent entre les États Chinois et Taïwanais, ou même entre Israéliens et Palestiniens, ou plus récemment les Géorgiens et les Russes. Les attaques se caractérisent par le piratage de systèmes informatiques, des attaques rendant les réseaux vulnérables, la défiguration de sites web. Mais aussi des attaques par déni de service ou « Denial-of-service », qui est une attaque visant à rendre muette une machine en la submergeant de trafic inutile. Il existe la possibilité que plusieurs machines soient à l'origine de l'attaque visant à anéantir des serveurs ou des sous-réseaux par exemple (on parlera d'attaque distribuée DDoS). Voici quelques exemples d'attaques par déni de services : les buffers overflows, l'attaque SYN, Teardrop, SMURF...²³ Elles sont le fruit de hackers (ou pirates informatiques) s'unissant pour attaquer un ou plusieurs sites gouvernementaux d'un État soit par conviction, ou par défi, comme une sorte de jeu qui engendre bien des conséquences. On pourrait parler selon Dorothy Donning d'« Hactivisme ». Ce terme est le fruit de la contraction des mots « activiste » et « hackers », et représenterait un ou des mouvements activistes qui utiliseraient les nouvelles technologies de l'information et de communication afin de véhiculer des revendications²⁴. À noter que porter atteintes aux intérêts de l'État en France est sanctionné notamment par l'article 323-1 du code pénal.

Ainsi il faut concevoir la protection du cyberspace comme l'espace aérien ou maritime.

Il convient de souligner que la France s'est dotée d'une infrastructure et d'équipements permettant de faire face à une guerre électronique. Ainsi il existe un Centre de direction et d'exploitation de la guerre électronique (CDGE), utilisant des outils technologiques tels que EMERAUDE (Ensemble mobile d'écoute et de recherche automatique des émissions). Celui-ci permet le brouillage des communications, l'interception de faisceaux hertziens analogiques, l'interception de transmissions de données etc..... Il se distingue du système d'espionnage américain ECHELON. Cependant la France serait dotée d'installations similaires surnommées Frenchelon et dont les stations seraient réparties sur l'ensemble du territoire, tant en métropole (comme par exemple à Domme dans le Périgord, le Mont Valérien, le plateau d'Albion...), qu'en outre mer (Tontouta en Nouvelle Calédonie, le centre d'écoute militaire des Bandamiers à Mayotte), voire sur des bases situées dans des anciennes colonies comme à Djibouti (base de Bouar).

Ces préoccupations de préserver l'intégrité du territoire et la sécurité des citoyens nous amènent à évoquer les mesures qui pourraient porter atteinte à notre vie privée.

En tenant compte d'un chiffre éloquent, et que nous devons apprécier avec un certain recul, 80% des informations utiles pour les services de renseignements américains tels que la NSA, seraient accessibles à partir de sources ouvertes.

Or on constate la volonté des militaires de la DRM (Direction du renseignement militaire) d'exploiter, de stocker et sauvegarder ces renseignements et les rendre interoperables (entretien de Michel Massion ancien directeur du renseignement militaire, jusqu'en 2008, général du corps aérien, publié dans le n°4 de Sécurité globale, Paris, Choiseul Juillet 2008, p9-18).

²³ : pour plus d'informations voir le site sur la sécurité informatique et des informations www.securiteinfo.com

²⁴ : Dorothy Donning, "Cyberwarriors, Activists and Terrorisms turn to Cyberspace", *Harvard International Review*, Summer 2001, p.70

Au regard des dangers existants sur le Réseau, l'État doit aménager des régimes d'exceptions à certaines libertés au regard des risques de tranquillité et de sécurité illustrée par la nécessité de l'ordre public.

Section 2 Risques et dangers du cyberspace

Au vu de la multitude des risques qui existent sur le Réseau, il semble légitime qu'un encadrement se fasse.

Ainsi la recherche de la « tranquillité » pour les utilisateurs d'Internet est primordiale.

En sachant que cette technologie n'est plus réservée à des militaires ou d'éminents informaticiens, mais à un ensemble d'utilisateurs qui sont parfois très jeunes.

Il existe de nombreux risques qui constituent une menace réelle du monde virtuel pour les plus jeunes.

Nous allons étudier une partie de ces dangers tant d'un point de vue humain que technique.

Cet outil interactif permet aux jeunes utilisateurs de se projeter dans un monde, qui devient un véritable mode de vie.

Toute la difficulté réside dans le fait de savoir distinguer ce qui est réel dans ce monde virtuel. Les jeunes n'ont pas souvent conscience de la notion de vie privée et de l'importance de la protection de cette dernière.

Ainsi ils n'hésitent pas à s'exposer sur des sites dits sociaux et ainsi faire part ouvertement de leurs vies.

Certes cela fait partie de la notion de liberté personnelle que nous avons vue, à savoir être libre dans sa démarche dans le cyberspace.

Cependant les parents ainsi que les administrations doivent sensibiliser leurs enfants sur de nombreuses questions.

Car une grande majorité d'entre eux remplissent des formulaires avec de nombreuses données personnelles leur permettant par la suite de participer à des concours ou des sondages.

Ces informations sont souvent données à des inconnus rencontrés sur des forums de discussions.

Ce qui les expose dans certains cas à des prédateurs sexuels sur Internet, se faisant passer pour des jeunes du même âge.

Ainsi ils arrivent, avec une certaine psychologie perverse, à entrer dans l'intimité de la vie d'un enfant manquant bien souvent de discernement, quant aux risques qu'il court.

Dans un autre cas moins grave quand à l'intégrité physique, ils peuvent être l'objet de cyberintimidation qui consiste en règle générale, en des menaces, ou des messages haineux envoyés par courriels.

Les jeunes sont exposés à d'autres menaces, comme le fait d'être exposé à des contenus violents, comme des images de tortures, des images pornographiques...mais aussi des contenus racistes, haineux, révisionnistes.

Ces sites et ces contenus peuvent heurter la sensibilité des jeunes et les influencer à un moment de leurs vies, où ils se cherchent et se construisent.

Enfin il ne faut pas oublier de mentionner les risques du fait de l'incitation à des jeux de hasard, qui peuvent par la suite créer une addiction. On note que ces sites sont relativement faciles d'accès et souvent anonymes.

Dans le but de préserver la « tranquillité et la sécurité » de ces jeunes utilisateurs, l'encadrement du cyberspace se justifie.

La pédopornographie constitue un des dangers du cyberspace, qui est un sujet mal connu sauf dans certains cas quand la presse en fait écho, et qui doit être durement réprimée. Dans la convention des droits de l'enfant des Nations unies, elle est définie comme «*toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles* ».

Le texte principal réprimant la pornographie infantile se fonde sur l'article 227-23 du code pénal « *Le fait, en vue de sa diffusion, de fixer d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende* ».

Ce qui peut poser problème dans la rédaction du texte, réside dans le fait que si la photo d'un mineur nu ne prenant pas une position ambiguë, lascive, à caractère sexuelle, ne peut rentrer dans le champ de la définition du code pénal.

Il existe une loi du 4 mars 2002 qui réprime aussi la détention d'images pornographiques d'un mineur, qui doivent être stockées dans le disque dur de la machine.

Du fait de son côté transfrontière, l'harmonisation des législations peut paraître parfois difficile, mais celle-ci n'est pas impossible comme nous le verrons ultérieurement.

Les risques qui circulent sur le Réseau n'affectent pas seulement les jeunes utilisateurs.

En effet, la sécurité et les services de l'État peuvent être concernés comme nous l'avons vu précédemment, tout comme une entreprise ou un simple particulier.

Les conséquences pour les différents utilisateurs peuvent être désastreuses.

Ainsi des mesures ayant pour but de divulguer des informations confidentielles ou même erronées peuvent porter atteinte à la réputation d'une entreprise et peut être favoriser ses concurrents.

Des attaques ciblées peuvent affecter sérieusement le fonctionnement d'un service, sans compter les risques d'accidents pouvant entraîner des drames humains (comme par exemple une attaque des services de contrôle aérien, ou de la gestion de l'eau d'une ville....).

Toutes ces mesures peuvent faire l'objet d'une malveillance particulière, grâce à certains programmes comme des virus affectant le fonctionnement de différentes machines.

Il convient de mentionner entre autre l'exemple des *logiciels espions (spyware* en anglais) collectant des informations personnelles et les renvoyant à une tierce personne.

Des logiciels *rootkit* qui permettent l'installation d'une porte dérobée, permettant d'obtenir des informations ou de les altérer sans laisser de traces dans le système de la machine infectée.

L'enregistreur de frappes (keylogger) est un programme qui à l'insu d'un utilisateur enregistre les frappes du clavier.

Le cheval de Troie (Trojan) apparaît à l'utilisateur comme un programme légitime, mais qui exécute des tâches nuisibles.

Ceci ne constitue pas une liste exhaustive de programmes malveillants existants sur le Réseau, mais sont en règle générale les plus courants.

D'autres dangers sont caractérisés par des attaques sur le Réseau comme le *sniffing*, qui permet l'identification des machines sur le Réseau et par la suite de récupérer les mots de passe.

La *mystification (spoofing)* est une technique généralement utilisée afin d'obtenir des informations sensibles en prenant l'identité d'une machine ou d'un utilisateur. Il convient de noter que l'usurpation d'identité peut être sanctionnée selon l'article 423-23 du Code Pénal de cinq d'emprisonnement et de 75 000 euros d'amende. D'autres types d'attaques visent les messageries en se propageant grâce à des programmes malveillants.

Ce sont le plus souvent des *pourriels (spams)*, ils se caractérisent par le fait que le courriel n'est pas sollicité, son contenu a pour objet de faire la publicité, ils encombrant le Réseau, et font perdre du temps et surtout de l'argent aux entreprises. Au travers de machines zombies des millions d'adresses vont se générer et ainsi expédier une masse consistante de messages.

Il existe un principe d'interdiction énoncé à l'article L121-20-5 du code de la consommation : « *Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.* »

L'*hameçonnage (phishing)* est aussi un courrier électronique ayant pour but d'obtenir des informations confidentielles grâce à la substitution d'identité (comme par exemple le cas du remplacement d'une page d'un organisme bancaire afin d'obtenir les données bancaires de la victime).

Il existe bien d'autres types d'attaques, mais ces dernières sont moins courantes et nécessitent certaines compétences techniques. Comme par exemple le *cassage de logiciels (cracking)* qui permet la modification d'un programme afin de contourner les éléments permettant sa protection.

On constate qu'il n'y a pas vraiment d'harmonisation en terme de législation concernant les risques liés au Réseau.

Cependant depuis le 1er juillet 2004, un premier texte européen sur la cybercriminalité a été adopté par nombre de pays dont la France, qui permet de compléter les législations internes souvent peu élaborées concernant les problématiques posées par Internet et les nouvelles technologies.

Ce texte permet de renforcer les capacités policières dans les investigations et la collecte de preuves.

Il convient de noter qu'un Protocole additionnel relatif à l'incrimination d'actes raciste et xénophobe au travers d'Internet complète l'acte précédent.

On remarque que la France a ratifié ces deux textes par la loi n°2005-493 le 19 mai 2005.

Ce qui nous amène à nous intéresser à la législation encadrant le cyberspace et les outils permettant cette sécurisation.

Chapitre 2 Vers une sécurisation nécessaire de cet espace

Afin de lutter contre les nouvelles formes de criminalité favorisant l'insécurité, l'État doit modifier le cadre juridique de la politique de sécurité, par des outils juridiques adaptés, mais aussi par des outils technologiques.

Section 1 La politique française de sécurisation et l'émergence d'une nouvelle régulation normative

Ce n'est que relativement récemment qu'une prise de conscience sur les enjeux du cyberspace est réellement apparue. Il est vrai que certaines lois prévoyaient des dispositions concernant la sécurité, et la sanction d'infractions au regard d'Internet.

On note que souvent les lois nationales sont souvent le fruit d'une transposition soit d'un accord international, soit de la transposition d'un texte communautaire.

Nous allons nous intéresser aux principaux textes internationaux, qui ont influencés la législation française.

Le traité de l'OMPI sur le droit d'auteur en date du 20 décembre 1996, énonce ainsi dans son article 4 l'obligation de protéger les « programmes d'ordinateurs en tant qu'œuvres littéraires ».

L'article 11 oblige les parties à sanctionner les personnes contournant des DRM.

L'autre texte majeur à l'échelle internationale, est la convention de Budapest, du 23 novembre 2001, et qui traite de la cybercriminalité.

On y retrouve les principaux dangers qui existent sur le cyberspace.

Ce texte apparaît clairement comme l'outil permettant une harmonisation des législations, s'unissant pour lutter contre les risques existants sur le Réseau.

Ce texte est des plus complets sur le fait qu'il saisit les enjeux d'une politique commune d'encadrement du cyberspace, mais qui ne soit pas trop attentatoire à certains droits.

Ainsi on remarque la nécessité de lutter contre le hacking (article 2), la pornographie infantile (article 9), ou les atteintes à la propriété intellectuelle (article 10).

Mais ce traité est soucieux par exemple que les données ne soient interceptées que sous certaines conditions comme le degré de gravité de l'infraction (article 21).

Tout comme la plupart des lois, les directives concernant le cyberspace, ou les impacts d'Internet sur des branches du droit, comme avec la propriété intellectuelle, sont assez récentes.

Mais au regard de la rapidité du développement de l'architecture du Réseau et des diverses incidences sur les droits et libertés, les textes même récents peuvent apparaître parfois inadaptés.

Il convient de citer la directive dite EUCD (european copyright directive) 2001/29/EC en date du 22 mai 2001.

Elle porte sur l'harmonisation concernant le droit d'auteur, et elle pose le copyright comme un droit général.

On constate que cette directive a été transposée en France par la loi DADVSI.

On y retrouve des éléments du traité de l'OMPI comme l'interdiction de contourner les DRM (article 6), le fait de porter atteinte au copyright sera sanctionné, comme le mentionne l'article 7.

La question de la protection de la propriété intellectuelle est une des préoccupations qui apparaît le plus souvent dans la plupart des textes, comme par exemple la directive IPRED en date du 29 avril 2004.

Elle incite les États membres à prendre toutes les mesures afin d'encadrer et de protéger la propriété intellectuelle.

Ce qui implique de prendre des mesures à l'encontre « des personnes morales dont les services sont utilisés par les contrefacteurs.... »

Enfin une des directives les plus importantes est celle appelée « Data Retention » du 15 mars 2006 qui a pour but d'obliger chaque État à obliger les fournisseurs d'accès à conserver les données relatives au connexion, comme les adresses IP, la durée de connexion...

Ce qui nous amène à examiner les différentes lois nationales.

On remarque qu'une des premières lois en matière d'informatique date du 5 janvier 1988 relative à la fraude informatique, et traitait des peines encourues en cas de vols ou de destructions de données, et de l'interdiction de toute intrusion dans un système informatique.

La loi du 1^{er} août 2000 relative aux obligations des éditeurs de sites Internet impose certaines obligations comme l'obligation de retirer des contenus illégaux (pour les hébergeurs), de conserver des données permettant l'identification d'auteurs d'infractions. Il convient de constater que cette disposition revient dans la loi LCEN.

Il est intéressant de noter qu'il n'y a pas eu, comme on pourrait le croire, une activité normative conséquente sur un laps de temps élargi si on tient compte d'une des premières lois en 1988.

La multiplication de textes relatifs au cyberespace, liés aux notions de sécurité, d'économie numérique, ou d'enjeux culturels, s'est développée essentiellement depuis les années 2000. Alors devons-nous penser forcément à l'aspect négatif de cet accroissement ?

Plusieurs réflexions sont possibles.

Tout d'abord, elle peut s'expliquer par l'obligation de s'adapter aux développements de l'architecture et des moyens du Réseau.

Mais aussi par les problèmes liés à la sécurité, « l'ordre public virtuel », mais bien réel, au problème de la propriété intellectuelle et enfin à des enjeux économiques.

De plus, cette évolution s'accompagne aussi par la nécessité pour l'État et son administration de s'adapter aux réalités techniques et économiques.

Mais on peut se demander comment un État peut encadrer Internet, si l'administration n'est pas sensible, ou du moins « frileuse » face à l'utilisation des nouvelles technologies.

On peut analyser cet accroissement normatif par le fait sans doute de la modification de la position de l'État face aux nouvelles technologies et vers le développement d'une administration électronique, plus que nécessaire.

La loi relative à la sécurité quotidienne du 15 novembre 2001 n'était pas a proprement dite destinée pour Internet, mais quelques articles intéressants y font référence.

Comme l'article 29 sur la conservation de données demandé par l'autorité judiciaire.

À noter une des dispositions qui dispose que si les fournisseurs d'accès ne collaborent pas, ils encourent une peine d'un an d'emprisonnement, d'une interdiction professionnelle ainsi qu'une amende de 75000 euros.

L'article 30 fait référence à l'encadrement de la cryptologie que nous verrons un peu plus tard au cours de l'étude de la question de la vie privée.

La loi principale de l'encadrement juridique d'Internet n'est apparue qu'en 2004.

En effet, la loi LCEN « loi pour la confiance dans l'économie numérique » énumère essentiellement dans son article 6 les différentes obligations des hébergeurs.

Ils doivent notamment retirer les contenus illégaux, conserver des données permettant l'identification des auteurs, la déclaration de fourniture de cryptologie, ou retirer les contenus copyrightés entre autre.

Concernant des dispositions d'ordre sécuritaire, la loi d'orientation et de programmation pour la sécurité intérieure (LOPSI) du 29 août 2002 prévoit la fusion du STIC, fichier de la police nationale, avec celui de la gendarmerie (JUDEX), au sein d'un fichier commun dénommée ARIANE.

Un des aspects importants de cette loi consiste dans la possibilité « d'accéder directement à des fichiers informatiques et de saisir par la voie télématique ou informatique les renseignements qui paraîtraient nécessaires à la manifestation de la vérité ».

Nous n'évoquerons pas ici la loi liberté et création (Hadopi) ou la loi de 2004, car nous les verrons ultérieurement.

Nous nous attacherons à énoncer succinctement une loi importante au regard de la sécurité, la loi du 23 janvier 2006 relative à la lutte contre le terrorisme.

Cette préoccupation, nécessité de maintenir la sécurité, permet un certain régime d'exception dans la mesure où des documents peuvent être demandés par les agents de la force publique sans la requête d'un juge.

De plus, certains services de polices peuvent obtenir des données personnelles conservées par les hébergeurs.

Des innovations en matière de sécurité sont complétées par des dispositions de la loi du 5 mars 2007 relative à la prévention de la délinquance.

De nombreuses dispositions assez diverses renforcent l'aspect sécuritaire de l'encadrement d'Internet.

Ainsi les policiers peuvent se faire passer pour des mineurs afin de traquer les prédateurs sexuels sur le Réseau, mais aussi sanctionner la publicité non autorisée d'un casino, ou permettre la possibilité de collecte d'un traitement automatisé de données à caractère personnel afin de lutter contre l'absentéisme scolaire.

Certaines dispositions des lois en vigueur ou prochainement en vigueur vont assez loin dans le progrès technologique, mais sont/ou peuvent représenter un risque pour la vie privée.

Il est loin le temps où cette intrusion se caractérisait par la mise sur écoute d'un téléphone.

Désormais il sera possible d'espionner grâce à un logiciel espion, type cheval de Troie. L'utilisation de ce type de software permet un suivi bien plus large que le système d'écoute téléphonique.

Concernant la loi LOPSI 2, la notion de filtrage par les fournisseurs d'accès concernant les sites pédopornographiques paraît compréhensible, et doit être facilitée et justifiée au regard de la notion d'ordre public.

Ainsi la « Loppsi2 » prévoit une sorte de cyberperquisition, qui offrira la possibilité aux cyberpoliciers de capter à distance et en temps réels les écrans d'un suspect. Cette mesure sera selon le ministère de l'Intérieur, prévue dans des cas bien précis comme des cas de terrorisme, de pédophilie, ou de grande criminalité.

Sachant que ce procédé ne pourra pas être mis en œuvre uniquement qu'au travers d'une commission rogatoire d'un juge.

Cette garantie juridictionnelle permet quand même de s'inquiéter sur les possibilités de cybersurveillance des citoyens.

De plus, ce contrôle de l'État pose une troublante question d'ordre moral au regard de la capacité de ce dernier à contrôler cet espace.

Certaines infractions pouvant troubler l'ordre public justifieraient-elle un contrôle de cette envergure ?

On constate que ce système de suivi à distance a été rejeté par la Cour Suprême de justice allemande en 2007.

La mise en œuvre de cette politique sécuritaire suppose une mise à dispositions des forces de sécurité de moyens performants permettant de lutter contre toute forme d'insécurité.

Section 2 Les outils de cette sécurisation

Il existe de nombreux outils qui permettent la sécurisation que se soit au travers l'utilisation de fichiers, mais aussi de logiciels que nous verrons un peu plus loin. Il est indéniable que l'État dispose d'un grand nombre de fichiers de police et de renseignements.

Selon les rapports existants, il y aurait 58 (rapports Bauer disponible sur le site de la documentation française) fichiers utilisés ou en cours de création.

Ils se divisent en plusieurs catégories avec ceux à vocation administrative, à caractère judiciaire, et enfin ceux à vocation de renseignements.

On peut se demander si cette multiplication de fichiers ne favorisent pas des doublons, et donc le développement et le stockage de données inutiles, et présentant un risque au regard de leurs protections.

On constate que ces fichiers sont tenus de faire l'objet d'une mise en conformité au regard des règles de protection des libertés, comme le souligne l'article 21 de la loi n°2004-801 du 6 août 2004 « les responsables de traitements.....disposent d'un délai allant jusqu'au 24 octobre 2010. »

Nous nous intéresserons à certains d'entre eux, soit par rapport à leurs liens avec une actualité récente, soit par rapport aux conséquences de ces fichiers sur la question de la vie privée.

Nous allons principalement analyser certains fichiers de renseignements et des fichiers d'antécédents judiciaires.

Concernant ces derniers, il s'agira principalement de s'intéresser au STIC (Système de Traitement des Infractions Constatées), et du JUDEX (Système Judiciaire de Documentation et d'Exploitation) qui seront regroupés dans le cadre du projet ARIANE.

Ils regroupent un ensemble d'informations extraites de procédures de police judiciaire. Ils ont pour vocation première la constatation d'infractions pénales, le regroupement de preuves liées à ces infractions, ainsi que la recherche de leurs auteurs.

Ils permettent, dans une certaine mesure, d'effectuer des rapprochements entre différentes affaires, au regard des similitudes, ce qui facilite la recherche des auteurs multirécidivistes de crimes ou délits.

Ces fichiers sont indispensables au regard des évolutions de la criminalité, mais un encadrement est nécessaire, ainsi que des formalités de publicité.

Ce qui n'est pas forcément le cas pour certains fichiers de renseignements.

Cela s'explique pour des raisons de sécurité nationale, des missions de protection de la souveraineté nationale. Il convient dès lors d'apporter quelques précisions sur ces fichiers de renseignements.

La loi de 78 précise qu'il existe un régime dérogatoire concernant l'utilisation par la DCRI (Direction Centrale du Renseignement Intérieur) de fichiers de renseignements. Ce régime dérogatoire est prévu par les articles 30 I et 44 IV qui prévoient la non publication de l'acte de création d'un tel fichier et ce qui peut être un peu dérangent, l'absence de droit de contrôle sur place de la CNIL.

Ainsi, le fichier CRISTINA (Centralisation du Renseignement Intérieur pour la Sécurité du Territoire et des Intérêts Nationaux) est couvert par le secret défense ce qui a pour conséquence la non publication du décret.

Ce fichier est le fruit de la réorganisation des services de renseignements du ministère de l'Intérieur, survenue le 1^{er} juillet 2008. Son statut de fichier « de souveraineté » défini par l'article 26 de la loi du 6 janvier 1978, ne peut faire l'objet d'un contrôle sur place de la CNIL. Cependant, cette dernière s'est toutefois prononcée sur ce fichier en émettant un avis favorable, mais avec certaines réserves.

Comme le fichier CRISTINA, le fichier GESTEREX (Gestion du Terrorisme et des Extrémismes à potentialité violente) constitue un fichier de renseignements dont aucune durée de conservation fixe n'est prévue. Il prévoit la prévention des actes de terrorisme, la surveillance d'individus ou d'organisations qui par leur caractère radical ou leur mode d'action sont susceptibles de porter atteinte à la sécurité nationale.

Ces considérations qui tendent pour des raisons d'ordre public, à limiter les libertés personnelles sont justifiées au regard de la nécessité de sécurité.

Il convient de remarquer un élément important qui consiste en la possibilité d'un droit d'accès et de rectification garanti à chaque citoyen par les articles 39 à 41 de la loi de 1978.

Ce droit s'exerce évidemment par l'intermédiaire de la CNIL.

Il existe certaines garanties fondamentales quant à l'utilisation de ce fichier. Ainsi, seulement certains fonctionnaires habilités peuvent l'utiliser. Il n'est normalement pas interconnecté avec un autre fichier.

Toutefois un élément peut paraître gênant, dans la mesure où une donnée peut être conservée le temps nécessaire, eu égard aux finalités du fichier. Cet élément temporel, un peu vague quant à la conservation des données, peut être l'objet de certaines critiques.

Un autre fichier mérite qu'on y prête attention, dans la mesure où son prédécesseur avait suscité la polémique. En effet, de nombreux points du fichier EDVIGE avaient choqués l'opinion publique. Il a donc été l'objet d'un remplacement par le fichier EDVIRSP (Exploitation Documentaire et Valorisation de l'Information Relative à la Sécurité Publique). Ce qui est surprenant, c'est qu'il n'a pas fait l'objet d'une profonde modification.

Ce fichier est destiné à collecter, conserver et traiter des données concernant des personnes dont l'activité individuelle ou collective peut porter atteinte à la sécurité publique.

Mais aussi les personnes faisant l'objet d'enquêtes administratives afin de savoir si leur comportement n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées compte tenu de leur nature.

Il permet entre autres, la collecte d'informations faisant apparaître les origines géographiques, des signes particuliers, ou même les activités politiques, philosophiques, religieuses ou syndicales.

Une des garanties majeures concernant l'utilisation de ce fichier réside dans la durée limitée de conservation de données ainsi par exemple, cette durée est portée à cinq ans à compter de l'enregistrement ou de la cessation au titre duquel l'enquête a été menée.

De même, concernant les mineurs de treize ans et plus, ces données ne peuvent être conservées que trois ans après l'intervention du dernier événement ayant justifié un enregistrement à ce titre. Enfin, les données doivent être épurées et mises à jour régulièrement, ce qui fera l'objet d'un contrôle par la CNIL.

De nombreuses interrogations apparaissent au regard de la multiplication de ces fichiers, notamment quant à leurs utilisations, la conservation des données stockées, mais aussi leurs destructions quand ces derniers ne sont plus utiles à une procédure.

On peut se demander quelle est l'utilité de conserver des informations sensibles d'une personne, et ce si cette dernière est mineure au moment des faits.

On constate que la loi distingue bien la conservation dans le cas d'un mineur de treize ans ou de seize ans est différente.

Cela nous amène à évoquer le droit à l'oubli, cause qui justifie que les services de sécurité utilisant ces fichiers soient précautionneux, dans l'utilisation des données stockées.

Ainsi on constate que la CNIL recommande pour ce qui est de la constatation de l'utilisation du fichier STIC que certaines mesures soient prises, dans l'utilisation de ces fichiers.

On remarque que ce n'est pas la conception du fichier qui est remise en cause mais plutôt les formalités d'utilisations.

On constate que l'utilisation de ces outils n'est pas forcément adaptée à certains fonctionnaires au vu sans doute du manque de sensibilisation et de formation dans l'utilisation de ces outils.

En effet, la CNIL constate que certains fonctionnaires (bien trop nombreux ont accès à ces informations) sont peu précautionneux dans la mesure où les codes d'accès sont notés sur des feuilles accrochées aux ordinateurs.

Ainsi il conviendrait d'adopter des mesures d'habilitation, puis de traçabilité afin de sécuriser l'utilisation et le recours à ces fichiers.

D'autres graves irrégularités ont été constatées.

De nombreuses erreurs sont commises lors de la saisie du motif pour lequel la personne figure dans ce fichier.

Ainsi l'erreur est parfois faite entre la victime et le mise en cause.

D'autres problèmes ont été relevés notamment au regard de la conservation de données dans les bases locales dans la mesure où aucune purge n'est effectuée régulièrement.

Il convient de préciser que le fait d'être mentionné dans ce type de fichier emporte parfois de graves conséquences, comme par exemple le fait de se voir refuser un emploi. En effet, certaines professions notamment celles liées à la sécurité, imposent une autorisation administrative, délivrée par la préfecture (comme par exemple pour les emplois aéroportuaires).

La CNIL s'engage à effectuer un nouveau contrôle d'ici le 31 décembre 2011 afin de voir les modifications liées au précédent rapport²⁵.

Car au regard de certaines réactions et de l'émotion suscitée par le fichier EDVIGE, par exemple, démontre le problème de la transparence dans la création et l'utilisation de ces fichiers.

Ce manque de publicité, de clarté à l'égard des citoyens est critiquable dans la mesure où s'instaure un climat de suspicion à l'égard de tous les autres fichiers créés.

Ces questions de sécurité sont surprenantes au regard de leurs ambivalences et de leurs perceptions par les citoyens.

En effet, ces derniers réclament des mesures assurant leurs sécurités mais réagissent dès que certaines mesures sont prises.

Ce qui peut paraître comme une garantie contre l'utilisation excessive de ce fichier réside dans le fait du développement de la transparence de leurs utilisations.

Mais aussi du fait de la capacité de mobilisation des citoyens pour protester contre l'utilisation de certaines données par ces fichiers.

Et il est indéniable qu'Internet est l'instrument et le fondement de cette mobilisation citoyenne, assurant une « veille médiatique » quant à l'utilisation de fichiers, comme l'ont démontrées les protestations à l'encontre d'EDVIGE (exploitation documentaire et valorisation de l'information générale).

La polémique a poussé le gouvernement à retirer le fichier et le remplacer par EDVIRSP.

Comme nous l'avons vu, l'utilisation de ces fichiers s'avère nécessaire dans l'optimisation des ressources des différentes administrations, notamment la justice, et surtout les forces de sécurité.

Cependant au regard des progrès technologiques, on pourrait s'inquiéter de l'utilisation de certains logiciels.

En effet, le ministère de la Défense par le biais de la DGA (Délégation générale pour l'armement) s'est lancé dans un projet de surveillance des sources dites « ouvertes » numérisées baptisé HERISSON (« Habile extraction du renseignement d'intérêt stratégique au traitement des sources ouvertes »).

Ce système, portant un nom bien sympathique, permet de surveiller les informations qui circulent sur les réseaux de communications²⁶.

Il permet la recherche d'informations sur des protocoles de messagerie de type POP3 mais aussi des plateformes « pair à pair », les forums....

²⁵ : Rendu le 20 janvier 2009, consultable sur le site www.cnil.fr

²⁶ : voir article en date du 15 mai 2009 sur www.lemonde.fr

Il ne serait prévu que pour la recherche d'informations stratégiques sur des sources ouvertes, ce qui implique, qu'il n'affectera pas la sphère privée.

Mais comment en être sûr pour autant ?

Le plus inquiétant réside dans le fait qu'aucune autorisation n'a été demandée auprès de la CNIL.

Le ministère de la Défense se fonde sur le fait que le logiciel ne permettra pas la création de base de données, et que cet outil ne constitue qu'un démonstrateur technologique²⁷.

Un autre « super fichier » mérite notre attention, au regard des capacités à capter et regrouper des informations variées.

Anciennement baptisé Périclès, devenu par la suite AJDRCDs (application judiciaire dédiée à la révélation des crimes et délits en série), permettra en utilisant des informations légalement utilisables de débusquer des suspects, grâce à la capacité de recoupement instantané des ordinateurs.

Il semblerait que dans les dispositions du deuxième volet de la loi LOPSI, la garantie de ne pas utiliser ce logiciel serait justifiée que pour les crimes et délits d'au moins cinq ans de prison.

Le plus surprenant de cette application informatique consiste dans sa capacité à se croiser avec les fichiers de police, les bases de données d'autres administrations, ou des systèmes d'informations d'opérateurs de téléphonies ou d'établissements financiers.

Le tout fondé sur un système de réquisition judiciaire accélérée.

De quoi inquiéter un minimum si cet outil est contrôlé par un juge Burgaud.

Mais on peut se demander si à l'avenir l'utilisation de ces technologies ne sera pas détournée à d'autres fins.

Cela nous amène à nous interroger sur les questions des risques d'atteintes dont nous pouvons faire l'objet.

Quelles sont les garanties quant aux intrusions dans notre sphère intime ?

Internet, ce cyberspace synonyme de liberté semble parfois, sous l'impulsion de certains intérêts diminuer notre liberté personnelle.

²⁷ : voir article mars 2009 sur www.pcimpact.com

Titre II La conciliation entre l'ordre public et liberté

Chapitre 1 Une protection issue d'un large dispositif juridique

Cette technologie constitue pour bien des utilisateurs un monde inconnu, qui par insouciance, négligence, ou par malchance subissent par la suite des atteintes. Se pose alors le problème de savoir et quel est le degré de protection de nos données personnelles, et des risques liés aux atteintes à la vie privée.

Section 1 Notions et risques d'atteintes à la vie privée

La notion de vie privée apparaît il y a près d'un siècle dans un traité de 1888 d'un juge américain, Thomas Cooley qui énonçait le « droit d'être laissé en paix » (The right to be alone).

Cette notion s'inscrit dans le cadre du souci de la protection contre les atteintes à l'intégrité corporelle.

Puis cette expression est reprise dans un célèbre essai de Samuel D. Warren et de Louis D. Brandeis²⁸.

Ces derniers plaidaient pour la création d'un droit à la protection de la vie privée, afin d'empêcher la presse d'utiliser tout type d'éléments pouvant affecter la vie privée.

De nos jours, le statut de la protection de la vie privée revêt autant d'importance que le droit à la sécurité, voire plus, du droit à la vie.

Cette notion de vie privée est comparable à celle de l'ordre public dans la mesure où elle n'apparaît pas clairement définie, et elle devient tout aussi inépuisable.

La vie privée représente un espace qui constitue notre intimité, dans lequel notre liberté personnelle ne peut être limitée et dans lequel ni l'État, ni personne ne peut y avoir accès.

Il convient de voir comment apparaît cette notion dans les différents textes, ce qui nous permettra d'essayer de la définir.

Tout d'abord il convient de citer l'article 9 du code civil qui précise que : « *chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à*

²⁸ : Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", 4 *Harvard Law Review*, 1890, p.193 à 204

empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnée en référé. »

On retrouve aussi la notion de vie privée dans le code pénal à l'article 226-22 « *le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »*

Cette notion apparaît aussi à l'article 226-1 de ce même code, qui porte sur la volonté de porter atteinte à la vie privée d'autrui sous n'importe quel procédé, est sanctionnée par une amende et une peine pouvant aller jusqu'à un an de prison.

On constate qu'il existe certes certains textes prévoyant la protection de la vie privée, mais pas forcément sa définition.

En règle générale, elle se définit de manière négative, à savoir est privé, ce qui n'est pas public.

Mais différentes composantes y sont intégrées, comme la vie familiale, sentimentale, la santé, les convictions religieuses, philosophiques...

Le problème majeur est de savoir comment garantir cette vie privée au regard des nouvelles technologies.

De même, quand elle doit se concilier avec des impératifs de sécurité, comme avec le cas des fichiers informatiques.

Cette conciliation entre l'ordre public et la liberté personnelle s'explique par la nécessité du respect et de la défense de la vie privée, mais aussi de la confidentialité de la communication.

Ce qui permet entre autre, et dans une certaine mesure d'échapper au contrôle étatique. D'où le conflit qui existe entre les États et certains utilisateurs d'un procédé de cryptologie et plus précisément de la cryptographie asymétrique.

Les États désirent mettre en œuvre un contrôle quant à l'utilisation d'un logiciel de cryptographie asymétrique dont ils détiendraient l'unique clef.

Cette emprise sur les logiciels de chiffrement comme par exemple le logiciel PGP (Pretty Good Privacy) ou sa version libre GNU PG peut poser un certain nombre de risques ou de préoccupations au regard de la vie privée ou de la liberté d'usage.

Le problème majeur pour un gouvernement réside dans le fait qu'il ne souhaite pas perdre le contrôle, et la possibilité de surveiller le Réseau.

Ainsi, il est plus facile d'effectuer un contrôle et de s'immiscer dans la vie privée et l'intimité d'un sujet au travers des nouvelles technologies, bien moins coûteux, que si il avait fallu intercepter et lire les lettres.

Il convient de noter que la loi relative à la sécurité quotidienne prévoit sur la base de l'article 30 de sanctionner le refus les chiffres permettant le déchiffrement par des peines allant de deux à cinq ans d'emprisonnement et d'une amende allant de 30 000 à 75 000 euros.

On peut s'inquiéter des risques d'intrusion dans la sphère privée du fait du progrès des nouvelles technologies, même si parfois les citoyens sont consentants à certains types d'intrusion.

Car il convient de remarquer, que contrairement à ce qui y paraît, personne n'est anonyme sur Internet, et laisse forcément des traces.

Cependant ce qui peut paraître choquant, réside dans le fait que parfois, les utilisateurs fournissent volontairement des informations pouvant sérieusement compromettre leur vie privée.

Ainsi par exemple de nombreuses entreprises proposent des services type « payez ce que vous conduisez » (pay as you drive ») comme les compagnies d'assurance Axa ou MMA en Italie.

L'argument majeur étant celui du prix se basant sur la façon de conduire.

Les voitures ainsi équipées d'une borne GPS transmettent en temps réel tous les déplacements du client, leurs kilomètres, leur vitesse²⁹.

Ce type de comportement des entreprises se fondant sur un argument choc, suscite quelques inquiétudes au regard des atteintes à la vie privée.

Des garanties sont offertes aux citoyens dans la mesure où ils peuvent par exemple consulter le site « service public », et notamment « les guides de la CNIL », qui permettent, au travers d'explications claires, les possibilités de défense en cas d'intrusion et d'atteintes à la vie privée, du fait d'un traitement informatique d'informations personnelles, collectées soit par une entreprise ou une institution.

Ainsi, il convient de noter le rôle majeur de la CNIL dont l'une de ses missions premières est de veiller à protéger la vie privée et les libertés individuelles.

Elle veille à ce que les informations utilisées dans un traitement automatisé de données soient « adéquates, pertinentes et non excessives par rapport aux finalités du traitement ».

De plus, elle propose au gouvernement les mesures législatives ou réglementaires de manière à ce que les libertés puissent être protégées au regard des évolutions technologiques.

Concernant l'organisation de la CNIL, on constate qu'il existe plusieurs services repartis en pôles.

Nous n'évoquons ici qu'à titre d'exemple les services qui intéressent l'objet de cette étude.

Concernant la direction juridique, il existe un pôle justice, police, droit d'accès indirect et libertés publiques.

De plus, on relève le rôle fondamental de la direction de l'expertise informatique et des contrôles, dans la mesure où il apporte de nombreux conseils dans la mise en place d'un traitement automatisé, ainsi que dans les dossiers de déclaration préalable.

Au sein de cette direction le service de contrôles veille à toutes les questions concernant la question de la coopération policière européenne relatives aux programmes Europol et Schengen.

Tout un symbole de garantie au rêve des polices européennes dans la volonté d'interconnecter les fichiers de police.

L'impact de la CNIL est important, et cette dernière le démontre par ses activités, et sa place au sein des différentes institutions.

En effet, de nombreux communiqués sont publiés tout comme différentes actions de sensibilisation sur la loi informatique et libertés, ainsi que des colloques.

On peut par exemple mentionner le peu de satisfaction des commissaires de la CNIL au regard de certains termes de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme.

On remarque ainsi que l'autorité de la CNIL est indéniable dans la recherche d'un équilibre entre la prévention et la répression, et surtout dans la préservation des différentes libertés.

Le fondement de la protection des libertés personnelles dans le cyberspace s'explique par le rôle de la CNIL et la loi de 1978, mais on peut se demander si cela constitue une réelle protection des données personnelles.

Ainsi on peut se demander si il existe des limites à cette protection.

²⁹ : DELARCE, Valérie, « Assurance : automobilistes sous surveillance », *Les Échos*, décembre 2006

Section 2 Quelle protection pour les données personnelles ?

L'utilisation d'Internet par un utilisateur, emporte un certain nombre de conséquences. En effet, celui qui au travers de certains actes conscients ou non, expose une partie de lui-même notamment au travers de ses données personnelles.

On constate que la tendance de nos jours est à la compilation et au traitement de données personnelles, car elle s'avère en règle générale peu onéreuse.

Cependant nous ne savons pas forcément quel sera l'usage de ces données personnelles. Il convient dès lors d'apporter quelques précisions sur cette notion.

On constate qu'à l'origine dans la loi du 6 janvier 1978 « informatique et libertés » ne concernait que les informations nominatives, mais grâce à une modification de la loi de 1978 par celle du 6 août 2004, le terme donné à caractère personnel est venu remplacer le précédent.

Ce qui permet par cet aspect plus vague d'opérer une extension de l'application de loi informatique et libertés.

Ce sont un ensemble d'informations qui permettent d'identifier directement ou indirectement une personne physique.

Elles correspondent en règle générale, aux noms, prénoms, date de naissance, mais aussi, à un simple numéro de téléphone ou à une adresse électronique.

On remarque que ces informations peuvent être laissées facilement soit au détour d'un courrier électronique, mais aussi d'un formulaire en ligne, ou plus simplement lors d'un achat sur un site web d'un cybercommerçant.

Se pose alors la question de savoir quel est le degré de la protection de ces données personnelles ?

Tout d'abord, l'utilisateur soucieux de la protection de ces données personnelles doit faire preuve de bon sens dans l'utilisation de ses données, dans sa navigation sur le réseau.

Concernant l'aspect moins pratique et plus juridique, il existe en France la loi informatique et libertés de 1978, qui a institué par la suite la Commission informatique et libertés (CNIL).

Des dispositions de cette loi ont été modifiées par la loi n°2004-801 du 6 août 2004 (J.O n°182 du 7 août 2004).

La préoccupation de protéger l'individu face au danger de l'informatique, a surgi dû à la révélation d'un projet du gouvernement de l'époque (1974), qui souhaitait interconnecter les fichiers de l'administration à partir d'un identifiant unique, sur la base du numéro de sécurité sociale (affaire SAFARI : Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus).

Ainsi, la France fut l'un des premiers pays soucieux de la protection des données personnelles.

Cependant, avant cette dernière, certains pays comme l'Allemagne en 1970 (c'est le Land de Hess qui adopte la première loi), s'est dotée d'une législation protectrice.

Mais on peut citer les exemples de la Suède en 1973, ou des États-Unis en 1974 avec le *Privacy Act*, concernant les fichiers des administrations fédérales.

Ainsi une évolution du processus de protection des données personnelles s'est accrue avec l'effet communautaire, et des directives comme celle du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation des données (Directive n°95/46/CE).

Concernant les modalités autorisant la création d'un système de collecte et de stockage de données, une déclaration auprès de la Commission nationale informatique et libertés doit être faite au préalable par tous organismes ou entreprises, à travers d'un responsable de traitement des opérations de collecte et d'enregistrement de ces données.

À la suite de la validation faite par la CNIL, sera attribué un numéro d'enregistrement qui devra être indiqué sur le site Web de la société, ou de l'organisme, ainsi que l'adresse de contact du service responsable de la gestion de ces données personnelles.

Il est important de souligner que toute personne doit être informée par le responsable du traitement de la collecte et de l'enregistrement de ces données, de la finalité du traitement, de l'identité du destinataire de ces informations, et surtout de ses droits (au regard de la loi informatique et libertés et plus précisément des articles 32 et 38).

Certaines données ne peuvent être collectées ou traitées au regard de notre législation, quand elles font apparaître les origines ethno raciales, celles relatives au sexe ou à la vie sexuelle, aux croyances religieuses ou philosophiques, et enfin les appartenances syndicales.

Ce qui nous amène à préciser que certains organismes sont dispensés de déclarations quand à l'inscription de leurs membres, comme par exemple les partis politiques, les associations ou les églises.

Il en va de même pour les sites Web des particuliers, si cette activité est strictement personnelle.

Les données médicales constituent aussi des données personnelles, et ne peuvent être collectées que dans des cas bien précis, comme dans le cas du dossier médical personnalisé.

La condition fondamentale dans la gestion de ces données par les professionnels de santé consiste dans le fait de les anonymiser.

À noter que la mise en place d'un traitement de données personnelles sans que celui-ci soit autorisé, est durement sanctionné par le code pénal au regard de l'article 226-16 : «Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende... » Cependant la puissance publique grâce à la traditionnelle préservation de l'ordre public justifie l'atteinte à la protection des données.

Mais on constate que les données personnelles font l'objet d'une sérieuse protection, qui s'accroît au travers du rôle de la CNIL.

Cette dernière constitue une réelle garantie dans le domaine du contrôle des applications de l'informatique.

Cette autorité indépendante dispose d'une large palette de mesures dissuasives allant d'un simple avertissement, que d'une mise en demeure ou une injonction de cesser un traitement automatisé de données. Enfin le pouvoir de sanction le plus dissuasif étant les sanctions pécuniaires.

Elle a aussi vocation à conseiller tant les administrations, que les entreprises et les particuliers.

Ces derniers disposent d'une mine d'informations et de conseils comme le démontre la facilité d'accès du site Internet.

Il convient de remarquer qu'avant la loi du 12 mai 2009 tendant à la simplification du droit et l'allégement des procédures, les actes préparatoires de la CNIL n'étaient pas rendus

publics, le deviennent désormais, ce qui constitue une garantie pour les risques d'atteintes aux libertés.

Mais de nombreuses interrogations subsistent au regard de certains aspects techniques. En effet, l'utilisateur d'Internet lors d'une connexion laisse des traces numériques.

Celles-ci sont constituées d'un ensemble de fichiers qui s'enregistrent sur l'ordinateur de l'utilisateur, et souvent à son insu.

En règle générale, il s'agit de cookies, de formulaires, de fichiers Internet temporaires...

Il convient de noter que ces traces peuvent s'effacer assez facilement avec un logiciel type Internet explorer ou Fire Fox.

Mais il est intéressant de se demander si un cookie peut être considéré comme une donnée personnelle.

Car ce dernier permet de suivre les habitudes de navigation de l'utilisateur, en opérant une collecte d'information.

À noter que récemment la Cour de Cassation s'est prononcée sur le fait de savoir si une adresse IP pouvait constituer une donnée personnelle.

Dans sa décision du 13 janvier 2009, la chambre criminelle de la Cour de Cassation estime que les procès verbaux dressés par des agents assermentés pouvaient parfaitement se passer d'une autorisation de la CNIL.

Il semblerait qu'une adresse IP ne soit pas une donnée personnelle.

Or la question est de savoir si l'adresse IP doit être considérée comme une information qui permet d'identifier une personne indirectement ou non et ainsi savoir si elle est une donnée à caractère personnel.

Cette adresse IP se décompose en une série de chiffres, qui permettent d'identifier un ordinateur sur le Réseau.

Ce n'est que là qu'apparaît la complexité de la question juridique.

Dans la mesure où cette adresse IP identifie des machines et non une personne.

Car le propriétaire de la machine n'est pas forcément le responsable d'une faute quelque soit.

On relève par cette décision une dissension entre la conception de la CNIL, qui prévoit qu'en cas de collecte d'adresses IP, une demande doit être faite, et la position de la Cour de Cassation. Cette dernière ne se prononce pas directement sur la nature juridique de l'adresse IP. Cependant elle refuse d'admettre la position et la qualification des juges du fond, qui considèrent l'adresse IP comme une donnée personnelle, et dont la collecte devait faire l'objet d'une autorisation par la CNIL.

D'autres problématiques peuvent paraître comme des limites à cette protection comme par exemple les obligations imposées par la loi pour la confiance dans l'économie numérique (LCEN) et plus particulièrement les procédures de signalement.

Il n'existe pas d'obligations générales de surveillance des données.

Cependant les fournisseurs d'accès et les hébergeurs doivent signaler les comportements illicites (article 6-1-7 LCEN).

Ce sont différents types de données comme celles permettant d'identifier l'abonné, les adresses IP, les données permettant d'identifier les destinataires des communications....(voir décret d'application du 24 mars 2006).

Ces considérations techniques nous amènent à constater, que dans une certaine mesure la question de la protection des données peut se voir affectée par la question de la sécurité, qui amènent à la prise de dispositions sécuritaires, comme avec les cas des passeports biométriques ou les mesures concernant les PNR.

Le passeport biométrique a été instauré par un décret en date du 30 avril 2008.

Il convient de remarquer que la CNIL n'était pas favorable à ce type de document sans la mise en place d'un débat parlementaire.

Concernant l'aspect technique, ce document est équipé d'une puce RFID (radio frequency identification) dans laquelle sont enregistrées une photo et les empreintes digitales de deux doigts.

Enfin pour conclure sur ce chapitre, les données des dossiers passagers (PNR), posent un certain nombre de problèmes au regard de la protection des données personnelles, ainsi que de la vie privée.

Ces données constituent un ensemble d'informations qui ont fait l'objet d'un accord entre les États-Unis et l'Union européenne concernant les voyageurs entre ces continents, dans le cadre d'échanges d'informations.

Le problème majeur pour la CNIL et ses homologues regroupés au sein du G29, réside dans le fait que les Américains sont moins inquiets par la protection des données personnelles, surtout quand il est question d'assurer sa sécurité.

Cependant ceci laisse craindre une sorte de surveillance généralisée dans laquelle nos données peuvent être collectées en toute impunité, et sans réelles protections quant à l'utilisation de ces dernières par le gouvernement américain.

Comme nous l'avons vu précédemment la question du téléchargement présente plusieurs difficultés d'ordre technique et juridique.

Cette décision, qui concernait le problème du téléchargement par un internaute et l'échange de titres musicaux protégés par la SACEM, illustre le problème de l'apparition d'un ordre public culturel sur Internet.

Chapitre 2 L'impact d'un ordre public malléable

Jusqu'à présent nous nous étions préoccupés ou du moins intéressés plus à la notion de sécurité liée à l'ordre public, mais la polémique que suscite la loi liberté de création ou plus communément appelée HADOPI, nous amène à réfléchir sur l'émergence d'un « ordre public culturel » qui pose de nombreux problèmes au regard de la propriété intellectuelle mais aussi au regard des enjeux économiques.

Mais quid de ma liberté ?

Section 1 Vers un ordre public culturel ?

Comme nous l'avons vu, la malléabilité de l'ordre public a été la cause de l'apparition de nouvelles préoccupations comme en matière sociale, ou même éthique comme avec la décision de l'assemblée du contentieux du Conseil d'État du 27 octobre 1995 « Commune de Morsang-sur-Orge » relative au lancer de nains.

Mais cette notion d'ordre public, qui comme nous l'avons vu est très extensible, a permis d'inclure dans le fameux triptyque de l'ordre public (sécurité, tranquillité, salubrité), une autre notion, celle de moralité.

Cette notion a permis d'interdire la sortie d'un film à caractère pornographique du fait de l'immoralité du film selon la Haute juridiction administrative dans un arrêt en date du 18 décembre 1959 « Société Les films Lutétia ».

Il convient de constater que la notion de bonnes mœurs a évolué depuis et ce qui pouvait être choquant hier, ne l'est plus forcément de nos jours.

Cette évolution des mœurs s'est aussi adaptée aux nouvelles technologies, qui ont bousculé de nombreuses conceptions.

Ainsi le développement des sites sociaux comme Facebook a changé le rapport à la notion de vie privée.

Ce qui nous amène à nous intéresser au bouleversement du monde assez figé de la culture par rapport aux nouvelles technologies.

La réflexion porte sur un aspect global d'une question majeure, illustrée par un problème d'actualité.

La question est de savoir si les mesures sont prises dans l'intérêt par exemple de la protection du patrimoine culturel, ou bien d'autres préoccupations.

Car Internet permet l'accès à la culture dans sa vision la plus « universelle », qui touche tous types de catégories de personnes, bien loin du « Siècle des Lumières », où la culture appartenait à l'élite des hommes détenant la connaissance et l'intelligence.

Il convient ainsi de réfléchir sur l'aspect relativement nouveau de l'apparition d'un ordre public culturel sur Internet notamment avec la fameuse loi Création et Internet, et la kyrielle de controverses qui s'ensuivent.

Cette loi a fait plusieurs passages devant différentes instances, comme à la CNIL, au Sénat, à l'Assemblée nationale (par deux fois) et au Conseil constitutionnel, qui l'a en partie censurée.

Il convient de remarquer que cette loi a comme la loi DADVSI connu de nombreuses difficultés quand à son adoption.

La loi relative aux droits d'auteurs et aux droits voisins dans la société de l'information du 1^{er} août 2006 est la transposition de la directive EUCD.

Comme la loi Hadopi, elle constitue une mesure afin de lutter contre le piratage, du moins essayer de le diminuer.

Ainsi elle contenait un dispositif de riposte graduée, qui au (oh !) grand hasard, a été censuré par le Conseil constitutionnel dans une décision en date du 27 juillet 2006, en vertu du principe de l'égalité devant la loi.

Comme pour Hadopi, il y a (on pourrait dire avait) une autorité de régulation des mesures techniques (AMRT).

On remarque une disposition tout aussi pédagogique comme l'illustre l'article 28, qui consiste à envoyer de la part des fournisseurs d'accès des messages de sensibilisation sur les dangers du téléchargement... ». On ne peut que constater son efficacité de nos jours.....

Il convient de s'intéresser à plusieurs points, et essayer de comprendre pourquoi cette mesure a déchaîné autant de passions.

Une des mesures principales de la loi est la création d'une autorité publique indépendante, la fameuse Hadopi (Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet).

Cette dernière disposait de la possibilité d'émettre une sanction, avec la mise en place de la « riposte graduée ».

La procédure était la suivante :

Dans la mesure où un utilisateur était repéré et l'infraction constatée (concernant le téléchargement), un premier courriel d'avertissement prévenait l'auteur de l'infraction.

En cas de récidive, une lettre recommandée était envoyée, puis en dernier ressort la coupure était ordonnée.

Il convient de noter que cette procédure, était selon la ministre de la culture de l'époque, Mme Albanelle, une mesure à « vocation pédagogique ».

Tout d'abord plusieurs aspects de cette mesure semblaient choquants.

En effet, notamment celle qui consistait à fournir l'adresse IP de l'abonné suspect de n'avoir pas surveillé sa machine, par un fournisseur d'accès chargé, d'identifier l'utilisateur, puis de procéder à la coupure.

Mais quelle garantie était offerte par le fournisseur d'accès pour pouvoir sans aucune certification ou gage de sécurité, officier cette coupure en utilisant certaines données personnelles.

De plus comment garantir que l'utilisateur téléchargeant, était bien le propriétaire de la machine mise en cause. Car cette dernière peut être le fruit d'une utilisation collective.

Ainsi la sanction s'appliquerait à tous et pas seulement à l'auteur du téléchargement.

Mais en outre comme la plupart des offres Internet sont couplées avec la télévision et le téléphone, la coupure portait un préjudice d'ensemble, notamment celle de disposer du téléphone pour avoir la possibilité d'appeler les services d'urgence.

Enfin la loi prévoyait l'utilisation d'un logiciel de sécurisation installé sur la machine, payant et apparemment non interopérable.

Mais quelle certitude ou quelle garantie pour l'utilisateur que ce dispositif ne constitue pas un mouchard permettant le contrôle de la navigation sur Internet.

De nombreuses questions se posent, notamment d'ordre moral, au regard de la volonté de l'État de contrôler un peu plus ce sujet.

De plus cette loi n'offrait pas énormément de garantie au propriétaire de la machine, du respect des droits de la défense entre autre.

Une des critiques émises est celle posée quant au problème de renversement de la preuve prévue à l'article 1315 du code civil et pose le principe, que la preuve incombe au demandeur.

Cependant de nombreux aspects de cette mesure pédagogique semblaient poser certains problèmes comme l'a d'ailleurs bien soulevé le Conseil constitutionnel dans sa décision du 10 juin 2009.

Il constate en se fondant sur l'article 11 de la Déclaration des droits de l'Homme et du Citoyen (« la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme... »), qu'Internet constitue un instrument d'une liberté, et il ne pourrait s'en voir privé que par un juge.

Ainsi la commission des droits de la Hadopi, autorité non judiciaire, ne peut déconnecter un internaute du Réseau (concernaient les articles 5 et 11).

On remarque dans cette décision du Conseil des Sages, valide une partie du projet de loi, cependant avec certaines réserves, notamment dans le fait que le traitement de données devra faire l'objet d'une autorisation auprès de la CNIL.

De plus, les filtres proposés devront être fournis par un « pouvoir réglementaire », et non par Hadopi.

Le Conseil valide dans sa décision le fait de créer des labels pour les moyens de sécurisation. Cependant cela n'a pas pour effet de faire de cette possibilité une condition à l'obligation de surveillance de l'utilisateur.

Il semblerait au travers de cette analyse que l'obligation de surveillance quant au devoir de surveillance de la machine soit plus importante que l'objet de la loi, qu'est le problème du téléchargement.

La loi a été finalement promulguée le 12 juin 2009, mais on peut émettre certains doutes quant à l'avenir, et aux fonctions de cette autorité.

Avant les vacances parlementaires d'été, la deuxième version du texte était à l'étude, et le vote repoussé pour le mois de septembre.

Il semblerait que le nouveau ministre de la culture M. Mitterrand est tenu compte de la censure partielle de la première version de la loi.

Ainsi par exemple au travers d'une procédure simplifiée et par un juge unique des sanctions pourront être prononcées.

Les ordonnances pénales pourront prononcer des amendes ou la coupure d'Internet.

De même l'utilisateur manquant à l'obligation de surveillance de l'accès Internet pourra faire l'objet d'une sanction pour « négligence » et réprime par une amende et ou une coupure de sa connexion pour une durée maximum d'un mois.

Il convient de préciser qu'à ce jour les mesures peuvent de nouveau faire l'objet d'une saisine auprès du Conseil Constitutionnel.

On constate que cette démarche et cette politique diverge quant à la position communautaire sur le sujet.

En effet, le Parlement européen a adopté une posture bien différente sur la base du rapport « renforcement de la sécurité et des libertés fondamentales sur Internet » en date du 26 mars 2009.

La démarche européenne est claire dans son opposition à l'encontre de toute sanction de privation d'accès à Internet.

De même, on peut réellement s'interroger sur l'efficacité d'une telle mesure. Cette dernière n'aura vocation qu'à poursuivre, en règle générale, de jeunes utilisateurs. Il n'est pas trop compliqué d'un point de vue technique de contourner ce dispositif en utilisant par exemple des proxys anonymisants et payants, soit par le biais d'un réseau (privé)VPN, ou bien même via le streaming.

Cependant il faudrait plus penser à ce genre de dispositif pour lutter contre les organisations criminelles, et la lutte contre le blanchissement d'argent, notamment vis-à-vis de nombreux sites de jeu en ligne.

En outre, on peut craindre que la mise en place de ce dispositif, afin de « préserver » la culture ne soit l'occasion de pouvoir étendre encore plus le contrôle de l'État sur le cyberspace.

Il est évident qu'Internet a profondément modifié l'approche des utilisateurs au regard de l'activité culturelle et des usages culturels.

Ce bouleversement provoque irrémédiablement une mutation des industries culturelles, qui face à une situation d'urgence au regard des pertes financières liées au téléchargement, s'en

remettent à des projets normatifs de différents gouvernements, ayant pour principales vocations, la sanction de certains comportements.

Ainsi il convient de mentionner une condamnation historique qui a été prononcée en Suède à l'encontre des administrateurs d'une plateforme de téléchargement illégal The Pirates Bay, poursuivis pour complicité de violation de droits d'auteurs, et condamnés à un an de prison et 2,8 millions d'euros de dommages et intérêts³⁰.

Mais on peut se demander quel va être l'impact de cette décision au regard des nombreuses plateformes qui existent, ainsi que de leurs utilisateurs.

Ces derniers utilisent ces plateformes, comme par exemple Rapidshare, Mininova, Megaupload ou même The Pirates Bay pour s'échanger des fichiers qui sont protégés par le droit d'auteur. Elles permettent de rediriger leurs utilisateurs vers les fichiers (films, musique, logiciels....) détenus et mis à dispositions par les particuliers.

Il faut noter que la liberté d'expression, qui constitue une liberté fondamentale, tend à favoriser l'accès à l'information, comme le souligne la décision du Conseil constitutionnel. La sanction imposant une coupure constitue une limite au droit de chaque utilisateur d'avoir un droit d'accès au Réseau, outil de cette liberté d'expression.

Mais il est évident que le problème posé par la loi création et Internet, remet en cause la notion de droit d'auteur telle que nous la connaissons.

Cette dernière semble mal adaptée à l'ère numérique et la réelle préoccupation est bien la rémunération de l'auteur ou le créateur de l'œuvre originale et non celle de ceux qui en font le commerce.

Dans cet aspect numérique des entreprises ont su tirer profit par rapport à la vente du contenu numérique comme la société Deezer, mais aussi les fournisseurs d'accès.

Mais on peut se demander si il existe un droit de diffusion d'une œuvre en particulier, de la culture ?

Car dans l'état actuel des choses l'utilisateur ayant vocation de partager certaines œuvres rares et méconnues du public risque une sanction dans l'échange et la mise à disposition de cette culture.

Ce qui nous amène à essayer de réfléchir à de nouveaux concepts, de nouveaux moyens permettant à la fois l'accès à la culture de forme universelle au travers du cyberspace, mais aussi à la préservation de la créativité et de l'originalité des artistes par la rémunération juste de ces derniers.

On peut se demander quel type d'exploitation viable est faisable ou possible par l'artiste.

Ainsi la nécessité de préserver de nombreux intérêts comme les droits d'auteurs ou même la diversité culturelle impose de nouvelles solutions.

³⁰ : *Le Journal du Dimanche*, 3249, 19 avril 2009, p.37

Section 2 Pour une conciliation des différents intérêts

Une conciliation entre la propriété intellectuelle et la diffusion d'une œuvre semble possible.

Il faut cependant réfléchir à comment concilier des intérêts qui peuvent parfois paraître bien opposés.

Ainsi il ne semble pas impossible de trouver une méthode qui concilie ces intérêts divergents, comme avec le cas du développement du concept du « shareware », qui s'utilise pour les logiciels. Un utilisateur peut se servir d'un programme afin de l'essayer, et l'auteur ne sera rétribué que s'il s'en sert réellement.

Il convient dès lors de voir si le cas de la licence globale, du logiciel libre peuvent représenter une alternative.

Le concept du logiciel libre se fonde sur la possibilité donnée à chacun d'utiliser, de modifier, de diffuser ce logiciel.

Mais on peut se demander si ce modèle est viable quant aux créateurs, et si ils existent des risques d'une réutilisation lucrative du logiciel.

Il convient de préciser que Richard Stallman a été le premier à formaliser la notion du logiciel libre, qui a été ensuite popularisée par le projet GNU.

On constate que bien qu'il existe une apparente liberté, l'utilisation de ce type de logiciel est cependant encadrée, ce qui constitue une sorte de protection juridique de type droit d'auteur.

En effet, l'auteur y intègre le copyleft (licence de type GPL) au logiciel libre.

Il permet certes le partage, mais il rend le logiciel moins libre lors de sa redistribution.

De plus, le code source devra être accessible tant pour le logiciel original, que pour les modifications apportées.

Alors on peut se demander comment survivent les auteurs de ces logiciels.

Ces derniers ne tirent pas profit de la vente des logiciels mais des services associés au logiciel.

On peut donner pour exemples quelques logiciels libres connus du grand public comme linux, le navigateur web Mozilla Firefox...

Concernant la musique, à la suite des débats sur Hadopi, un collectif a soumis la perspective d'une licence globale, qui permettrait de financer en partie la musique sur Internet.

Pour résumer, la proposition de ce collectif se baserait sur une somme modique payée par l'utilisateur, qui lui permettrait de télécharger sans limitations particulières, et d'échanger. Cependant on peut se demander sous quelle base la répartition se ferait entre les auteurs, les producteurs....

De plus comment pourrait se faire l'évaluation, c'est-à-dire sur quels critères pour savoir comment rémunérer les artistes. Ceux qui seront l'objet de plus d'écoute et de téléchargement ?

De même réfléchir sur un mode de rémunération solidaire qui soit inclus dans le prix que nous payons aux fournisseurs d'accès. À noter donc qu'il existe un vrai droit fondamental de l'accès au Réseau.

Ainsi on constate que des solutions sont possibles, tant d'un point de vue financier, que juridique.

Il faut sans doute travailler sur l'adaptation du droit d'auteur aux nouvelles technologies.

En effet, ce droit est fortement discuté dans la mesure où parfois l'originalité peut être remise en cause, comme par exemple dans le cas de la stratégie commerciale de Microsoft.

L'utilisation du cyberspace doit se faire de manière concertée dans la mesure où les États, les entreprises et les cybercitoyens ont l'obligation de s'entendre afin d'éviter que cet espace ne se limite, voire disparaisse dans le format tel que nous le connaissons.

De plus l'évolution des moyens des technologies de l'information et des communications bouleverse la conception classique, avec l'utilisation du WIFI, la RFID (radio frequency identification)....

Ainsi l'ère que nous connaissons actuellement est cruciale dans le développement d'Internet et des nouvelles technologies.

Ces dernières favorisent l'interopérabilité comme avec le développement de terminaux polyvalents, qui permettront à l'avenir de fonctionner sur les réseaux cellulaires et sur les réseaux locaux. Il paraît possible que se développent des moyens pouvant obtenir de hauts débits sur des courtes distances avec l'utilisation de l'ultra large bande (UWB).

Ce qui d'une certaine manière oblige le droit à s'adapter.

Il suffit de voir la migration du support dans l'utilisation d'Internet et les enjeux qui s'ensuivent.

Jusqu'à présent la connexion au Réseau se faisait dans une majorité de cas à partir d'un poste fixe.

Désormais celle-ci est possible grâce à la téléphonie mobile.

Or il y a environ 1,5 milliards d'utilisateurs d'Internet, et plus du double si on tient compte de l'accès par un téléphone, soit environ 3,8 milliards de personnes.

Alors c'est toute une conception dans l'utilisation d'Internet qu'il faut concevoir.

Ceci tant d'un point de vue de la sécurité du Réseau, des États ou des personnes, que de la législation qui le régit ou de l'économie numérique.

L'un de ces facteurs d'adaptation est justement l'ordre public, qui doit réguler, légalement le Réseau.

Cet outil de la sécurisation est sécuritaire dans la mesure où il affecte les politiques publiques de la régulation.

Cet ordre public malléable, permet comme nous l'avons vu au cours de cette étude, de s'adapter aux circonstances.

Cette adaptation à cette évolution pourrait se concevoir par la codification de l'ensemble des textes, tant internationaux, que communautaires que nationaux.

On ne doit pas concevoir cet encadrement seulement d'un point de vue interne.

Cependant, il est difficile de croire que près de 250 États puissent se mettre d'accord sur des questions diverses comme la dignité humaine ou le révisionnisme.

Car cet ensemble de textes parfois disparates ne favorise pas la lisibilité de l'encadrement du cyberspace.

Il pourrait ainsi contenir les dispositions assez diverses, allant du téléchargement et de la nouvelle conception du droit d'auteur lié au numérique, que de l'utilisation de la cryptologie, comme le problème de la pédopornographie.

L'encadrement de l'architecture d'Internet doit se fonder sur un concept d'ouverture, car un des problèmes majeurs est la possibilité d'une crise, illustrée par la perte de confiance dans le Réseau, ce qui affecterait l'économie numérique, et bien plus encore.....

BIBLIOGRAPHIE

- AAVISKO, Jaak, “Real Threats From The Imaginy World”, *Vital Speeches of the Day*, Janvier 2008, p.28
- BIGO, Didier, *Polices en réseaux : l'expérience européenne*, Paris : Presses de la Fondation nationale des sciences politiques, 1996, 358p.
- BIGO, Didier, « Sécurité et immigration : vers une gouvernementalité par l'inquiétude ? », *Cultures & Conflits*, 31-32, 1998, p. 13-38
- DELARCE, Valérie, « Assurance : automobilistes sous surveillance », *Les Échos*, décembre 2006
- DONNING, Dorothy, “Cyberwarriors, Activists and Terrorisms turn to Cyberspace”, *Harvard International Review*, Summer 2001, p.70
- HUYGHE, François-Bernard, *L'ennemi à l'ère numérique : chaos, information, domination*, Paris : Presses universitaires de France, 2001, 211 p.
- HUYGHE, François-Bernard, « L'information, c'est la guerre », *Panoramiques*, 52, Corlet, 2001
- LEBRETON, Gilles, *Libertés publiques et droits de l'Homme*, Paris : Armand Colin, 2005, 551 p.
- LUCHAIRE, François, *Naissance d'une constitution, 1848*, Paris : Fayard, 1998, 274 p.
- ORWELL, Georges, *1984*, Paris : Gallimard, 1972, 438 p.
- PÉGUY, Charles, *Les Cahiers de la quinzaine*
- PICARD, Étienne, « Les restrictions exceptionnelles aux libertés publiques », *Cahiers français*, numéro 296, mai-juin 2000
- PICARD, Étienne, *La Notion de police administrative*, Paris : Librairie générale de droit et de jurisprudence, 1984, 926 p.

- LIANG, Qiao et XIANGSUI, Wang, *La Guerre hors limites*, Paris : Rivages, 2003
- SAYAH, Jamil, *Droit à la sécurité et libertés publiques, Les États face à la sécurité*, PUG 2003
- HUYGHE, François-Bernard, *Quatrième guerre mondiale : faire mourir et faire croire*, Paris : éditions du Rocher, 2004, 236 p.
- HARVEY, Robert et VOLAT, Hélène, *USA Patriot Act : de l'exception à la règle*, Paris : Lignes, mars 2006, 215 p.
- VALO, Martine, « Biométrie, extrême fichage : danger ! », *Le Monde*, 16 septembre 2006
- VEDEL, Georges, *Droit administratif*, Paris : Presses universitaires de France, 1982, 174 p.
- WARREN, Samuel D. and BRANDEIS, Louis D., "The Right to Privacy", *4 Harvard Law Review*, 1890, p.193-204
- WEBER, Max, *Le savant et le politique*, Paris : Plon, 1959, 232 p.
- WIENER, Norbert, *Cybernetics, or Control and communication in the animal and the machine*, Paris : Hermann, 1948, 195 p.
- *Le nouveau Petit Robert de la langue française 2008*, Paris : Dictionnaires Le Robert, 2007, 2837 p.
- *Le petit Larousse illustré 2009*, Paris : Larousse, 2008, 1889 p.

Sites Internet

- www.courdecassation.fr
- www.conseil-etat.fr
- www.conseil-constitutionnel.fr
- www.cnil.fr
- www.interieur.gouv.fr
- www.defense.gouv.fr
- www.culture.gouv.fr
- www.assemblee-nationale.fr
- www.senat.fr
- www.legifrance.gouv.fr
- www.lemonde.fr
- www.lefigaro.fr
- www.pcimpact.com
- www.securiteinfo.com