UNIVERSITÉ de LILLE 2

FACULTÉ
DES SCIENCES JURIDIQUES
POLITIQUES ET SOCIALES

Années 2000 / 2001

DESS Droit & Cyberespace

http://www.droitetinternet.com/

Système Echelon
&
Programme Carnivore

Sébastien BENARD
Laetitia CHEVALIER
Marc JULIEN
Mathias MOULIN
Judicaël PHAN

Sous la direction de Monsieur le Professeur Jean-Jacques LAVENUE

Cours : Internet et Droit international ; ordre public interne et ordre public international

SOMMAIRE

II / Quelles limites à la surveillance globale à l'international et en interne ?

A / Les atteintes aux droits des autres Etats

1/ L'Etat et le droit international confronté à la suppression des frontières et à l'instantanéité en matière d'interception

a) Des interceptions continues et transfrontières en violation des accords internationaux …

b) … engendrant une remise en cause de la conception traditionnelle des compétences et de la souveraineté des Etats

2 / Quels impacts sur les alliances internationales économiques et militaires ?

a) Les alliés d'hier sont-ils les ennemis d'aujourd'hui ?

b) Echelon : Les moyens d'une tyrannie totale à la portée des USA

B / Les atteintes aux droits des personnes privées

1/ Une remise en cause des libertés fondamentales des individus

a) Le difficile respect des législations

b) Les tentatives de lutte contre les atteintes

2/ les atteintes aux droits des entreprises

a) de l'espionnage militaire à l'espionnage économique…

b) …en violation des principes internationaux de régulation du commerce

INTRODUCTION

En écrivant son célèbre « 1984 », en 1949, Georges Orwell n'était peut être pas un écrivain aussi précurseur que l'on a pu alors le penser. En effet son roman, qui décrit un monde où chaque fait et geste des citoyens est épié et connu par une autorité centrale, voit certains de ses aspects se réaliser aujourd'hui, au travers de systèmes nationaux et internationaux de télésurveillance. Et Georges Orwell n'était pas en avance sur son temps, car ces systèmes de surveillance existent depuis plusieurs dizaines d'années.

En effet, c'est depuis la naissance de la radio que l'interception des signaux, internationalement appelé SIGINT, pour Signals Intelligence, a débuté. Aujourd'hui, plus de 30 pays utiliseraient de tels systèmes Sigint d'interception. Ces systèmes permettent de capter tous les signaux, ceux des radars ou des missiles par exemple, mais ils permettent surtout de capter toutes les communications. Il effectuent alors ce qu'on appelle le COMINT, ou Communication Intelligence. Ce Comint permet l'interception secrète des communications étrangères et est défini par la NSA comme : « l'ensemble des informations techniques et des renseignements détournés des communications étrangères par une autre voie que leur médium ordinaire »[1]. A l'origine les cibles du Comint étaient les messages militaires et diplomatiques entre les capitales et leurs missions à l'étranger. Puis, dans les années 1960, avec l'accroissement des échanges commerciaux, le Comint est de plus en plus utilisé pour le renseignement à caractère économique. Plus récemment, on l'utilise pour la lutte contre le trafic de drogue, le blanchiment d'argent ou le crime organisé.

La mise en place du plus important Comint, réseau d'interception des communications, a débuté dès 1948. L'année précédente, l'URSS avait refusé l'aide du plan Marshall Américain, qui proposait d'aider les pays détruits par la guerre à se reconstruire et se redresser financièrement. C'est alors le début de la Guerre Froide. Dès 1943, les Etats-Unis et la Grande Bretagne s'étaient allié dans un réseau de renseignement appelé «Brusa Comint », en vue d'espionner l'Allemagne Hitlérienne. Après la fin de la guerre, ce pacte est renommé UKUSA, à partir des initiales des deux pays membres. C'est la naissance du UKUSA Security agreement. Les deux Etats créent par ailleurs des instances pour gérer ce pacte :

- *Aux Etats Unis*, le Pentagone crée d'abord l'AFSA (Armed Forced Security Agency), qui devient en 1952 la NSA (National Security Agency), basée à Fort Georges Mead, et dont l'existence ne sera révélée à la population que 10 ans plus tard. Le rôle de la NSA est de faire du contre-espionnage, de protéger les communications gouvernementales, mais elle effectue également des missions d'espionnage puisque l'on sait qu'elle a permis l'infiltration des communications des Nations Unies lors de la guerre du golfe.
- *En Grande Bretagne*, c'est le GCHQ (Governement Communication Headquarters), à Cheltenham qui collabore à l'UKUSA.

Le rôle principal de ces agences est d'écouter les émissions et communications stratégiques que s'échangent les Etats majors des armées du bloc communiste et desquelles on déduit leurs capacités militaires sur le terrain. Le Pacte est donc un outil mis en place pour traquer « le péril rouge ».

Rapidement, le pacte original va intéresser d'autres candidats. C'est ainsi que les deux fondateurs sont rejoints par le DSD (Defense signals directoral) Australien, le CSE (Communication security Establishment) Canadien et le GCSB (Governement communication security Bureau) Néo-zélandais, 3 services de renseignement à but militaire. Plus tard, d'autres pays tels que la Norvège, le Danemark, l'Allemagne ou la Turquie, ont signé des accords Sigint secrets et devinrent des participants tiers au réseau UKUSA.

Ce pacte UKUSA devient le système Echelon au cours des années 1970. En 1972 le témoignage d'un ancien employé de la NSA est publié dans la revue américaine « Remparts ». De plus en plus d'agents de la NSA et du CGHQ vont d'ailleurs se mettre à parler des dérives de ce système d'écoutes généralisées, malgré l'obligation de confidentialité et les risques d'un procès qui pèsent sur eux. Selon le général Michael Hayden, directeur de la NSA, plus de 7000 des 38 000 employés ont quitté l'agence ces dernières années, et il est impossible de les réduire tous au silence.

Jusqu'en 1995, aucun Etat membre ne reconnut l'existence du système Echelon. Cette année là le gouvernement Canadien déclara « collaborer avec certains de ses plus proches et plus anciens alliés pour l'échange de renseignements extérieurs (…) ». La révélation officielle de l'existence du système Echelon n'est néanmoins apparue qu'en 1998, lors de la déclassification de documents secrets par la NSA. C'est à cette date que les gouvernements européens ont fait semblant d'être surpris par l'existence d'un tel système de surveillance planétaire généralisé, et ont commencé à enquêter.

Ces derniers n'ont plus seulement été surpris, mais offusqués lorsque le journaliste britannique Duncan Campbell a rendu son rapport au Parlement Européen. En effet il y révélait que la plupart des écoutes étaient désormais réalisées dans un but commercial. Echelon, d'abord conçu pour « espionner » des cibles militaires, a été reconverti, après l'effondrement du bloc communiste, vers des objectifs civils.

On peut effectivement parler de fausse surprise des Etats Européens. D'abord de nombreux témoignages avaient révélé dans la presse l'existence d'un système international d'écoutes généralisé sous la direction des Etats-Unis, mais surtout les moyens techniques nécessaires à ce dispositif sur toute la planète ne pouvaient pas passer inaperçus. Toutes les communications sont susceptibles d'être captées par ce système : téléphone, fax, e-mail…etc. Les communications qui passent par câbles ou fibres optiques sous-marins sont écoutés depuis des années.

[1] Directive n°6 sur le renseignement, Conseil de sécurité Nationale des Etats-Unis, 17 février 1972.

Mais c'est surtout le dispositif de plus de 120 satellites qui peut difficilement rester caché. Ceux-ci captent les communications, quelle que soit leur nature, puis les renvoient vers les « grandes oreilles », d'immenses paraboles de 30 m de diamètre disséminées sur la planète depuis 1971.

Le système fonctionne par mots-clés. Il isole les données qui comportent ces mots-clés et les transmet aux services de renseignement qui sont alors chargés de les interpréter. Le système Echelon est ainsi capable d'analyser les 15 Go de messages électroniques et d'échanges sur les forums de discussion transmis chaque jour via Internet. La NSA traiterait en temps réel 1000 milliards de bits. Le système aurait une capacité de stockage de 90 jours, soit une mémoire d'1 téra-octet. Les 5 Etats du Pacte se répartissent la tâche : La NSA « espionne » les communications des deux Amériques, l'Angleterre celles de l'Europe et de l'Afrique, Le Canada les latitudes polaires et nordiques, l'Australie et la Nouvelle-Zélande celles de l'Asie et du Pacifique.

A l'intérieur de leurs frontières, les Etats-Unis ont choisi de développer un autre système afin de surveiller les communications : c'est le système appelé Carnivore. En effet, avec le développement de l'Internet, le gouvernement a décidé de se doter, en février 1997, d'un outil permettant d'intercepter tous les paquets de données électroniques échangées par des abonnées Internet : les e-mails, tous les fichiers transférés, les URL visitées…etc.

Le premier système était appelé Omnivore et fonctionnait sur un Solaris X86. Cette première version aurait coûté 900 000 $. En juin 1999 une nouvelle version, dénommée Carnivore, a été mise en place, fonctionnant sous Windows NT cette fois. Cette adaptation technique était nécessaire compte tenu du mode de fonctionnement de Carnivore : celui-ci se présente comme un PC que le FBI branche, après autorisation judiciaire, sur les serveurs d'un fournisseur d'accès Internet.

Chargé d'un logiciel conçu par le FBI, le PC lit le nom des destinataires et des expéditeurs ainsi que l'objet de tous les courriers passant par les circuits du provider, et ne retient, selon le FBI, que les messages suspects. Il utilise des filtres prédéfinis en fonction de la nature de l'écoute. En théorie, Les interceptions sont autorisées par un juge et ne peuvent intervenir que pour des crimes spécifiques et particulièrement graves.

La révélation de l'existence de ce système a été faite en décembre 1999 par un avocat dont l'un des clients, fournisseur d'accès à Internet, s'était vu imposer un système de surveillance des courriers électronique sur ses serveurs. Il a alors été révélé que le système était capable d'intercepter bien plus que les seuls messages provenant ou en direction d'une cible unique, comme l'avait affirmé le FBI.

Les associations de défense des droits civils telles que, notamment, l'EPIC (Electronic Privacy Information Center) et l'ACLU, voyant une atteinte certaine à la vie privée, se sont alors saisies de l'affaire.

Les Etats Unis semblent donc capables de surveiller toutes les communications, sur et en dehors de leur territoire. Echelon symbolise leur volonté d'instaurer un contrôle mondial, les Etats Unis s'affirmant toujours plus dans leur rôle de « gendarme du monde », sans toutefois pouvoir cacher des objectifs purement mercantile,s et la fin de la guerre froide entraînant un glissement de la surveillance vers la sphère économique et donc civile.

La « découverte » d'Echelon met les Pays Anglo-Saxons face au reste de la communauté internationale, tout comme Carnivore met le Gouvernement américain face au jugement de ses citoyens.

On peut cependant estimer que la surveillance, voire la télésurveillance, est nécessaire à la sécurité nationale. Mais si la surveillance par l'Etat de son territoire se justifie au regard de l'ordre public interne, elle doit néanmoins respecter les droits fondamentaux des individus, du moins dans une démocratie.

En outre, la mise en œuvre d'une surveillance à l'échelle mondiale par un Etat ou un groupe d'Etats porte atteinte à la souveraineté des Etats tiers et aux droits de leurs citoyens.

Comme nous le verrons, les systèmes de surveillance globale, c'est à dire qui visent tous les émetteurs et tous les récepteurs, sans distinction technique, ni de nature, tels Echelon ou Carnivore, semblent faire des émules tout autour de la planète, ce qui augmente l'enjeu des deux questions principales qu'ils posent :

- quelles sont les nouvelles limites apportées à la compétence et à la souveraineté des Etats ? Leur compétence accrue en interne leur offrent un contrôle global de la diffusion sur le territoire, alors même que leurs souveraineté et compétence sont diminuées vis à vis de l'extérieur puisque un contrôle global de ces émissions peut être effectué par un tiers et sans qu'il n'y ait de sanction effective.

- dès lors, comment définir et faire respecter un ordre public international garantissant la souveraineté des Etats et les droits des individus ?

Ainsi, si les Etats, au travers de l'exercice de leur souveraineté nationale, ont un droit légitime de surveiller les communications qui transitent sur leur territoire voire en dehors de celui-ci (**I**), ce droit possède cependant des limites sans lesquelles de graves atteintes sont portées tant aux droits des autres Etats qu'à ceux des personnes privées (**II**).

I / La surveillance, un exercice légitime et conditionné de la souveraineté nationale

La surveillance électronique est un exercice légitime de la souveraineté nationale si elle est exercée à l'intérieur du territoire national. Cependant l'espionnage hors du territoire national ne rentre pas dans les compétences étatiques.

A / Surveillance étatique à l'intérieur du territoire national :

L'Etat en qualité de souverain peut surveiller les communications électroniques transitant sur son territoire. Cette surveillance est encadrée juridiquement mais les moyens techniques et informatiques (Carnivore et ses avatars) à la disposition des autorités gouvernementales offrent la possibilité de gargantuesques dérives.

1/ « Souveraineté territoriale » et surveillance nationale

L'Etat peut-il légitimement surveiller sur son territoire les communications électroniques ?

L'Etat est *« une collectivité qui se compose d'un territoire et d'une population soumise à un pouvoir politique organisé »*.[2] Le territoire est donc l'un des éléments constitutifs de l'Etat. Il se compose de l'ensemble du territoire terrestre, y compris les voies d'eau, certains espaces maritimes (eaux intérieurs, mer territoriale) et l'ensemble de l'espace aérien (couche atmosphérique surplombant le territoire terrestre et maritime de l'Etat)[3]. Selon la coutume internationale (« pas d'Etat sans territoire »), l'Etat qui perd la totalité de son territoire perd sa qualité d'Etat.

L'Etat *« se caractérise* (également) *par la souveraineté »*[4], que les juristes allemands définissent comme la compétence des compétences *(Kompetenz-Kompetenz)*[5]. L'Etat est l'unique sujet de droit international à bénéficier de cet attribut fondamental[6], qui lui confère le « pouvoir juridique (...) de connaître une affaire, de prendre une décision, de régler un différend » [7].

Sur son territoire, l'Etat en tant que souverain peut exercer l'ensemble des compétences qui découlent de sa souveraineté. On parle alors de « compétence territoriale majeure » ou de « souveraineté territoriale » par facilité de langage. Les caractéristiques de la souveraineté territoriale ont été dégagées de la sentence rendue par Max Weber, arbitre unique de la Cour Permanente d'Arbitrage dans l'affaire de l'Ile des Palmes opposant les Etats-Unis aux Pays-

[2] Com. arb. Yougoslavie, avis n°1, 29 novembre 1991, et avis n°8, 4 juillet 1992.
[3] Nguyen Quoc Dinh, Patrick Daillier, Alain Pellet, Droit international public, L.G.D.J., 1992, 4è édition, 1269 pages, n° 270.
[4] Com. arb. Yougoslavie, avis n°1, 29 novembre 1991, et avis n°8, 4 juillet 1992.
[5] Selon la théorie du *territoire titre de compétence* de Radnitzky, le territoire constitue un titre juridique indispensable à la compétence étatique.
[6] Nguyen Quoc Dinh, Patrick Daillier, Alain Pellet, Droit international public, L.G.D.J., 1992, 4è édition, 1269 pages, sp. p. 394.
[7] Dictionnaire de la terminologie du droit international, *Sirey*, p. 132.

Bas. La souveraineté territoriale est l'indépendance de l'Etat à exercer, en exclusivité, sur son territoire les fonctions étatiques, à condition de respecter le droit international.

L'Etat a également compétence pour exercer ses attributs sur les sujets se trouvant sur son territoire (dans le respect des règles de droit international). La surveillance relève en effet des « fonctions étatiques » de l'Etat, à condition qu'il n'agisse pas de manière abusive ou arbitraire. Des règles juridiques encadrant la surveillance électronique au niveau national et international se développent. Cependant nous verrons en *infra* que ces règles peuvent être détournées de leur but.

2/ les bases légales de la surveillance

Le but invoqué par les Etats pour légitimer la surveillance électronique est la lutte contre la cybercriminalité[8] : terrorisme, pédophilie, trafic de stupéfiants, évasions fiscales, etc. La surveillance est légitime si elle est encadrée par des normes conformes au droit international, et si elle est exercée de manière non arbitraire et/ou abusive dans le respect des droits fondamentaux.

Les lois relatives à la surveillance électronique puisent leur philosophie dans le cadre juridique des écoutes téléphoniques.

a) Cadre juridique des écoutes téléphoniques

♦ Les écoutes téléphoniques en France et aux Etats- Unis

→ Cas de la France :

Le secret des correspondances en France, qui dérive directement du droit au respect de la vie privée, couvre les correspondances postales, mais aussi correspondances téléphoniques et par toute correspondances émise par un moyen de télécommunication (téléphone, minitel, télex, e-mail).

Il faut que le message soit privé, c'est à dire destiné à une ou plusieurs personnes, physiques ou morales, déterminées

Les interceptions peuvent d'abord être ordonnées par une autorité judiciaire. Plusieurs conditions sont nécessaires :

- Etre en matière correctionnelle ou criminelle
- Que la peine encourue soit supérieure à 2 ans
- Que l'Interception soit prescrite par un juge, qui contrôle aussi le déroulement des opérations

[8] Selon le ministre allemand des Affaires étrangères, Joschska Fischer, la cybercriminalité coûte 50 millions d'euros par an à l'Allemagne.

- Que l'interception dure au maximum de 4 mois, renouvelables

Un PV doit être dressé avec la date et l'heure de début et de fin d'interception. L'enregistrement est placé sous scellé fermé. Seuls les enregistrements utiles à la manifestation de la vérité sont retranscrits. Les enregistrements sont détruits à l'expiration du délai de prescription de l'action publique.

La Loi du 10 juillet 1991prévoit également la possibilité d'effectuer des interceptions de sécurité. Ces interceptions sont justifiées par des motifs de sécurité, motifs légaux :

- Recherche de renseignements de sécurité nationale
- Potentiel scientifique ou économique
- Prévention du terrorisme, de la criminalité et de la délinquance organisée
- Prévention de la reconstitution de groupements dissous.

L'autorisation est de 4 mois renouvelables pour la même durée. Le 1er ministre décide de l'interception sur proposition du ministre de la défense nationale, de l'intérieur ou des douanes. La Loi 10 juillet 1991 crée une Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS). Son président est désigné par le Président de la République. Il est informé dans les 48 heures de toute interception. La commission peut adresser des recommandations afin de faire cesser une interception.

→ Cas des Etats-Unis

Aux Etats-Unis, la loi ne fait pas de distinction entre les écoutes judiciaires et les écoutes de sécurité. Le respect du secret des correspondance troue son principe dans le IVème amendement[9] qui protège les citoyens contre les perquisitions illégales.

Les écoutes doivent être autorisées par un juge, qui ne peut le faire que pour un crime spécifique et particulièrement grave. Elles sont limitées dans le temps, en général pour 45 jours, et les juges doivent demander tous les dix jours des informations sur les résultats des écoutes téléphoniques.

Les écoutes ne peuvent en outre pas être effectuées n'importe comment. Les services de police se doivent d'utiliser des filtres prédéfinis en fonction de la nature de l'écoute autorisée.

Selon les déclarations du FBI, son système d'écoute national, Carnivore, respecterait ces principes. En effet, en théorie, le FBI doit requérir un mandat du juge qui autorise l'installation du système Carnivore chez un FAI déterminé. Les écoutes seraient en outre très précises et ne permettraient de n'écouter que des messages très ciblés.

Il semblerait donc que les mises sur écoutes soient largement réglementées afin de protéger les intérêts des citoyens, que ce soit en Europe ou aux Etats-Unis. Mais on ne peut

[9] « The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizure, shall not be violated, and no warrant shall issue, but upon probable cause, supported by Oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

nier l'existences d'écoutes attentatoires à la vie privée. En effet, il a été prouvé que certaines autorités outrepassaient leurs droits. De plus, il existe, au plan international, un vide juridique n ce qui concerne le respect de la vie privée, vide qui laisse la porte ouvert à toutes sortes de dérives.

- Système européen des droits de l'homme

Un bref rappel de la jurisprudence de la Cour européenne des droits de l'homme en matière d'écoutes téléphoniques nous semble indispensable, dans la mesure où le projet de Convention international sur la cyber-criminalité est développé au sein du Conseil de l'Europe (voir *infra*).

Selon le juge européen[10], les écoutes téléphoniques étatiques sont autorisées à condition que le droit à la vie privée soit respecté[11]. Les interceptions doivent donc être prévues par la loi, être nécessaires dans une société démocratique, limitées pour les cas d'infractions graves, et proportionnées au but poursuivi.

De plus la Cour de Strasbourg exige que les écoutes téléphoniques ne soient pas générales mais ciblées, ce qui n'a pas toujours été prévu par le projet de convention de lutte contre la cybercriminalité développé au sein du Conseil de l'Europe.

b) Cadre juridique de la surveillance électronique

Il semble se dégager de nos lectures, un mouvement commun aux législations nationales. Ces dernières sont calquées sur le modèle américain qui imposent une collaboration entre les fournisseurs d'accès à Internet (FAI)et les autorités nationales.

Cette harmonisation internationale des législations en matière de lutte contre la cybercriminalité législative s'accélère au travers du Conseil de l'Europe, sous l'influence américaine.

- Niveau national

A titre d'exemple aux Pays-Bas, les FAI doivent conserver les données de connexion des internautes pendant au minimum un an[12]. En Grande-Bretagne, le RIP Act (Regulation of Investigatory Powers) d'octobre 2000 permet au gouvernement d'intercepter toute communication considérée comme suspecte.

En France, L'article 43-9 de la loi du 30 septembre 1986 relative à la liberté de communication, modifiée par la loi du 1er août 2000 prévoit une obligation de conservation

[10] Cour européenne des droit de l'homme, 6 septembre 1978, affaire *Klass c. Allemagne*.
[11] Article 8 de la Convention européenne des droits de l'home, mentionné dans l'article 6 du Traité sur l'Union européenne. Directives 95/46/CE et 97/66/CE.
[12] Le coût estimé depuis 1998 année d'entrée en vigueur du Telecommunications Act est évaluer à 500.000 francs par FAI.

des logs par le FAI[13] relatifs aux *« services de communication en ligne autre que de correspondance privée »*, dont seule l'autorité judiciaire peut demander la communication.

L'avant-projet de loi sur la société de l'information qui devrait être présenté en Conseil des Ministres avant la fin juin 2001, retourne la situation en imposant l'effacement des données dès que la communication est achevée. Son article 17 autorise « uniquement » la conservation de ces données *« pour les besoins de la recherche, et de la poursuite des infractions pénales »*, ou *« pour les besoins de la facturation et du paiement des prestations de télécommunications »*.

- Prise de position de la commission européenne

La Commission européenne, afin de ne pas laisser au Conseil de l'Europe l'entière maîtrise de la question de cybercriminalité au niveau international s'est prononcée sur le projet de Convention sur la cybercriminalité dans son avis 2/2001 du 22 mars 2001[14] et a émis des communications.

Elle a également mis en place un forum public sur les questions de cybercriminalité. Ce forum a réuni *« les différents services de maintien de l'ordre, les fournisseurs d'accès, les opérateurs de réseau, les groupes de consommateurs et les autorités responsables de la protection des données, afin d'améliorer le degré de coopération au niveau européen, et d' attirer l'attention du public sur les risques posés par des criminels sur l'Internet »*[15].

- Echec des négociations du G8

A l'issue du sommet du G8 sur la cybercriminalité de Berlin des 24, 25 et 26 octobre 2000[16] aucune position commune n'avait été arrêtée[17]. Le but principal de ce sommet était l'étude du projet de convention mondiale sur la cybercriminalité du Conseil de l'Europe, dont l'objet est d'harmoniser les lois nationales relatives aux crimes et délits informatiques.

Ce projet a été vivement critiqué par 28 ONG qui ont dénoncé le « sérieux danger » d'atteinte à la démocratie au travers du renforcement des pouvoirs de police dans la collecte des données personnelles[18].

---

[13] L'adresse IP de l'abonné ainsi que ses heures de connexion et ses actions effectuées (upload ou download sur un serveur FTP, les pages webs qu'il a visitées, etc.).

[14] Le Conseil des ministres avait voté une résolution en 1995 incitant les opérateurs Internet et de téléphonie mobile européens à mettre en place sur leurs réseaux des systèmes de surveillance électronique permanente et en temps réel.

[15] Notons que L'Institut européen des normes en télécommunication (ETSI) prépare le standard européen en matière de surveillance électronique.

[16] Deux autres réunions sur le sujet avaient précédé ce sommet : la conférence de Paris en mai 2000 et le sommet annuel du G8 à Okinawa au Japon.

[17] Le problème de l'uniformisation de la lutte contre la cybercriminalité au niveau international est double. D'une part, les Etats ont une conception différente des notions de liberté d'expression, vie privée, données personnelles, actes de cybercriminalité..... D'autre part, à une échelle internationale, la mise en place d'une police internationale spécialisée dans la lutte contre la cybercriminalité est nécessaire.

[18] Les ONG soulignaient que ce projet était contraire au projet de Charte Européenne des Droits fondamentaux (adopté au Conseil Européen de Biarritz). Par exemple, *« les articles 14 et 15 pourraient mener à l'exigence d'un accès gouvernemental aux clés de chiffrement et cela pourrait contraindre les individus à s'incriminer eux-*

Si aucune entente n'avait été trouvée au sein des réunions politiques du G8, une volonté commune semble se concrétiser dans le cadre juridique offert par le Conseil de l'Europe.

- La convention mondiale de lutte contre la cybercriminalité ou la légitimation de Carnivore

Le projet de convention internationale sur la cybercriminalité[19] a été développé au sein du Conseil de l'Europe par ses 41 membres ainsi que par des non-membres : Etats-Unis, Canada, Japon et Afrique du sud. Les négociations ont débuté officiellement en février 1997, et 25 versions de ce projet ont été proposées. La Convention pourrait être adoptée à l'automne prochain et les Etats membres ou non du Conseil de l'Europe seront invités à la ratifier avant la fin de l'année 2001.

Le projet comporte trois volets :
- la définition des types d'infractions informatiques,
- la définition des procédures judiciaires pour adapter les pouvoirs d'enquête (saisie et conversation des preuves),
- la coopération internationale en établissant un réseau de points de contacts.

Le projet de convention sur la cybercriminalité reprend sur plusieurs points la législation américaine en vigueur, en particulier la question de la collecte des communications par le FAI[20]. Le projet prévoit que chaque pays pourrait « contraindre les fournisseurs de services de collecter et d'enregistrer (...) le contenu de communications spécifiées transmises par voie informatique [circulant] sur son territoire »[21].

Le principe est le suivant : soit le fournisseur de service[22] collecte et conserve seul les communications, soit il est dans l'obligation de collaborer avec les autorités compétentes. Dans le second cas de figure des systèmes de type Carnivore seront installés chez le FAI. Nous retrouvons ici l'influence des négociateurs américains.

---

mêmes, ce qui pourrait bien être incompatible avec l'article 6 de la Convention européenne des droits de l'homme ».

[19] http://conventions.coe.int/treaty/FR/projets/projets.htm
Ce document, provisoirement intitulé « Projet de convention sur la cyber-criminalité » sera le premier traité international à s'intéresser, sous l'angle du droit pénal et des procédures criminelles, aux différents types de comportements délictueux visant les systèmes, réseaux et données informatiques ainsi qu'à tous les autres abus de même nature.

[20] D'autres points ont également soulevé la colère d'ONG ou d'associations : la volonté de suppression de la double incrimination, les atteintes possibles à la protection des données personnelles et au droit à l'anonymat.

[21] Ajoutons que si la collecte ou l'enregistrement doivent être effectués en temps réel, dans sa dernière version, le projet ne prévoit plus une obligation de surveillance générale au travers d'un enregistrement systématique et globale des données, conformément à la recommandation 3/99 du groupe de travail relative à la préservation des données de trafic par les fournisseurs de service Internet pour le respect du droit adopté le 7 septembre 1999 au sein du système communautaire. Une telle obligation serait par ailleurs en totale contradiction avec l'article 8 de la Convention européenne des droits de l'homme étudié en *infra.* Mais la simple mise en place de dispositif de type carnivore sur le serveur des FAI permet une surveillance générale de la part des autorités policières.

[22] 'Service provider' dans la version anglaise, ce qui comme le souligne le Securityfocus, implique *« toute entité publique ou privée qui fournit à des utilisateurs la capacité de communiquer par voie informatique ».*

Malheureusement il existe un risque que les Etats imposent la mise en place systématique de clones de Carnivore, sous prétexte que le système mis en place par le FAI n'est pas efficace. Il ne nous semble pas exagérer de l'affirmer, par analogie avec la mise en place imposée par le FBI de Carnivore à Earthlink qui avait pourtant proposé un système capable de collecter uniquement les données transmises et reçues par la personne visée et non celles de tous ses abonnés, voir *infra*.

3/ Moyens techniques de la surveillance électronique : Carnivore

Nous retiendrons le qualificatif de Carnivore mais il faut au préalable souligner que le FBI a rebaptisé Carnivore en DCS 1000 (Digital Collection System).

Le modèle en matière de surveillance électronique est ou sera donc l'installation (légale) d'un logiciel de type Carnivore, par l'influence américaine au cours des négociations au sein du Conseil de l'Europe et l'action sur le terrain de la CIA. Il nous faut donc étudier l'histoire et le fonctionnement technique de ce logiciel de surveillance électronique.

- Historique de Carnivore

L'existence de Carnivore a été révélée par le *Wall Street Journal* en en juillet 2000, suite aux révélations de l'avocat d' Earthlink, FAI n°2 aux Etats-Unis. En 1999, le FBI a installé sur les serveurs d'Earthlink un système de surveillance de courrier électronique nommé « EtherPeek ». Le motif invoqué était la surveillance d'un seul individu. Mais après vérification auprès du fabricant du logiciel (la société AG Group), le FAI a appris que le système permettait de surveiller la correspondance de tous ses abonnés. Le FAI proposa donc au FBI une solution maison qui autorisait seulement la surveillance de l'individu suspecté. L'agence fédérale accepta un temps cette solution puis insista pour installer son propre système, cette fois ci, le système Carnivore.

Le FAI s'adressa à la justice pour qu'elle se prononce sur la conformité de l'ordonnance d'installation de Carnivore à la loi sur la confidentialité des communications électroniques (Electronic Communications Privacy Act)[23] . Le tribunal maintenu l'ordonnance et Earthlink a été contraint de collaborer avec le FBI[24].

Les caractéristiques techniques de Carnivore expliquent en l'insistance du FBI.

- Fonctionnement de DCS1000 (ex-Carnivore)

[23] Le 2 octobre 2000, suite au recours en justice de l'organisation non gouvernementale (ONG) Electronic Privacy Information Center (EPIC), le FBI a déclassifié plusieurs de ses notes internes confirmant les capacités de Carnivore. Le FBI affirmait auparavant que Carnivore, et son prédécesseur : Omnivore, et ne lisaient que les en-têtes des e-mails.

[24] De nombreux FAI ont collaboré avec le FBI : par exemple, UUNet et MCI Worldcom.

Carnivore a été créé par la NSA. Il prend la forme d'un logiciel tournant sous Windows installé sur un pc chez le FAI. Il fonctionne comme une boite noire et permet la surveillance de toute communication électronique transitant par le FAI. Il surveille toutes les information numériques et peut en faire une copie à destination du FBI (courrier électronique, chat, FTP, forums de discussion, etc.). Il peut également reconstituer la navigation de l'internaute sur la toile[25], et se comporte comme un des «sniffers » utilisé par les pirates, pour obtenir les codes d'accès à un serveur par exemple. Il est capable de scanner des millions de messages par seconde[26].

Carnivore, à la différence des systèmes d'écoute téléphonique, ne surveille pas uniquement les communications de la personne suspectée mais également les e-mails de tous les abonnés au FAI. Il filtre toutes les informations transitant par le FAI pour, en théorie, ne retenir que les correspondances de la personne visée. Les filtres sont définis selon le mandat de la police américaine, mais leur définition peut être changée à distance sans même que le FAI ne s'en rende compte.

Selon le rapport d'EPIC[27], Carnivore «est capable de capturer et d'archiver tout le trafic non filtré sur le disque dur interne (...) » du PC sur lequel il est installé. Pour reprendre une image de Laure Noualhat[28], les obligations pesant sur les FAI équivalent à demander à un facteur de conserver les photocopies du courrier qu'il distribue.

De plus comme le souligne Peter Sachs, président du FAI Iconn pour que Carnivore puisse trier les messages et ne lire que les messages suspects, il doit tous les lire. EPIC affirme que Carnivore fait partie d'un ensemble de surveillance électronique plus vaste aux noms de code Dragon Ware et Dragon Net.

Les limites de Carnivore se situent dans le fait que l'information pertinente ne doit pas être perdue dans le « bruit ». Signalons à ce propos que la société Raytheon (société américaine spécialisée dans l'armement et la défense) commerciale depuis peu un logiciel plus puissant que Carnivore. Ce dernier est basé sur un système de mots clefs alors que SilentRunner utilisent des algotihmes plus évolués qui analysent les données sous 25 angles. De plus la totalité du trafic est copiée sur le disque local, et le logiciel analyse ensuite offline (hors-ligne) les données. 150 logiciels SilentRunner ont trouvé acquéreurs (entreprises ou agences gouvernementales américaines) et le prix de chaque licence oscille entre 180.000 et 475.000 francs français. Ajoutons que le but officiel du logiciel est de protéger et de surveiller le réseau local de l'entreprise.

- A chaque pays, son avatar de Carnivore

[25] Selon le cahier des charges, Omnivore devait pouvoir « écouter le réseau (Internet) et imprimer des e-mails en temps réel et les stocker, avec d'autres données, sur des bandes magnétiques de 8 millimètres ». Sa mise au point dans les laboratoires de recherche du FBI à Quantico (Virginie) a été estimée à 900 000 $, ce qui peut sembler sous-évaluer. Le programme Omnivore fut opérationnel en 1997 ; le 9 juin 1999 Carnivore a officiellement 'pris son relais' . Cette transition a été permise grâce au programme Phiple Troenix.

[26] Carnivore fonctionne sous Windows 2000 et le stockage est un disque Jaz d'une capacité de 2 Giga-octets.

[27] Voir II-A pour de plus amples détails sur ce point.

[28] Laure Noualhat, les fournisseurs d'accès ne veulent pas être des indics, 12 avril 2001, www.europa.int.eu.

Si Carnivore est configuré de façon inappropriée, il permet d'enregistrer tout le trafic qu'il surveille. De très nombreux Etats ont donc installé, souvent avec la participation de la CIA, des avatars de Carnivore sur leur territoire. Ils ont adopté ou adopteront des lois obligeant les FAI à collaborer avec la police en installant, souvent à leurs frais, des dispositifs de type Carnivore.

USA

En l'an 2000, la surveillance électronique représentait aux Etats-Unis 8% de la surveillance globale. En théorie les interceptions ne sont autorisées par un juge que pour des crimes graves et limitées dans le temps avec une demande du juge tous les 10 jours des informations relatives aux résultats des écoutes.

Selon le FBI, Carnivore aurait été utilisé dans le cadre légal et uniquement 25 fois, dont 16 fois en 2000. Il aurait permis de récolter des preuves dans 6 affaires criminelles et 10 affaires de sécurité nationale[29]. Ces chiffres ne reflètent certainement pas la réalité car il suffit à un agent du FBI de déclarer à un juge fédéral qu'une personne est susceptible de commettre un crime pour qu'elle soit surveillée. D'autant plus que le quotidien britannique The Register révélait que le FBI avait invoqué les risques encourus par le bug de l'an 2000 pour procéder de nombreuses opérations illégales de surveillance électronique.

UK

La Grande-Bretagne est le pays le plus surveillé électroniquement. Le Regulation of Investigatory Powers (RIP) ACT autorise l'installation chez le FAI du MI5, dispositif équivalent à Carnivore qui est relié directement au service secret anglais. La décision d'activer ces boites noires ne serait d'ailleurs pas du ressort du juge judiciaire mais du ministre de l'intérieur. Le coût de la mise en place de ces boites noires a été évaluées par deux chercheurs britanniques à 20 millions de livres.

Hollande

Le gouvernement hollandais depuis le mois d'avril 2001 exige que les FAI mettent à leurs frais un logiciel de type Carnivore.

Norvège

En Norvège, les services secrets ont mis en place à l'insu du Parlement Norvégien un système identique à Carnivore baptisé VDI. Officiellement le but est d'empêcher toute intrusion dans les réseaux des principales entreprises et administrations norvégiennes.

Japon

[29] La surveillance électronique aurait permis de récolter des preuves dans 25.600 affaires criminelles en 13 ans.

Sous le nom de « Tempory Mail Box » ou Kari-no-mail (boite aux lettres temporaire) la police japonaise au cours de l'année 2001 met en place progressivement un système de type Carnivore, pour un prix de 1,37 millions de francs par boite noire. Le Parlement japonais, devant lequel le 10 novembre 2000 la police a dévoilé son projet, souhaitait que le code-source soit divulgué. Les frais inhérents à cette mise en place seront à la charge des FAI. Ajoutons que le Wiretapping Act rend légal l'interception des communications électroniques au Japon et que les juges qui autoriseront les interceptions électroniques ne pourront les contrôler.

De plus les autorités policières japonaises veulent constituer une base de données de visages et des voix transitant sur le réseau Internet.

Nouvelle-Zélande

Deux lois en Nouvelle-Zélande légitiment les actions de surveillance électronique par la police. La première autorise la surveillance du courrier électronique et la seconde oblige les FAI à coopérer avec la police.

Pologne

A la fin de l'année 2000, le ministre polonais des affaires intérieures avait transmis à la Chambre des technologies de l'information et des télécommunications un avant projet de loi obligeant tout hébergeur de données de s'équiper de dispositif de type Carnivore. En Pologne la polémique sur la question de la vie privée ne pose pas dans la mesure où les organisations de protection des droits de l'homme sont peu influentes. Le problème est œlui du coût de la mise en place d'un tel système qui risquerait de ne pas laisser la possibilité de survivre aux petits fournisseurs d'accès. En effet les FAI devront mettre en place à leur frais l'avatar polonais de Carnivore.

Russie

En Russie un système de type Carnivore répondant au doux nom de Sorm a été mis en place depuis plus de deux ans. Si le FAI ne veut pas collaborer, il perd sa licence octroyée par le gouvernement lui permettant d'exercer sa profession[30].

Inde

Le 17 octobre 2000 a été voté une loi indienne obligeant les FAI à collaborer avec les autorités indiennes en installant sur leurs serveurs un logiciel de type Carnivore. Par ailleurs cette loi a créé un tribunal spécial pour les affaires relevant d'internet.

[30] Une licence étatique est également nécessaire pour ouvrir un site Internet en Russie.

- Alternative et solutions ?

« Altivore » *:*

Une des raisons invoquées par Donald Kerr, directeur adjoint du FBI, pour ne pas révéler les sources de Carnivore est que la connaissance du code-source permettrait une utilisation malveillante par un détournement du logiciel. Pourtant il existe des clones de Carnivore disponibles en open source, comme Altivore (« Alternative to Carnivore ») de la société éditrice de logiciels Network ICE Corp. L'utilisation d'un tel logiciel par un FAI peut être un argument commercial envers une clientèle effrayée par le Carnivore, mais surtout ce logiciel traite uniquement que les e-mails (ce qui risque de limiter son nombre d'acquéreurs…).

Solutions :

Selon deux chercheurs britanniques[31], les systèmes de type Carnivore peuvent être facilement détournés par des criminels avertis. Par exemple : utiliser une connexion Internet via des comptes de téléphones cellulaires anonymes prépayés, certains types de cryptage, le recours à un petit fournisseur d'accès indépendant (le problème est de savoir s'il est réellement indépendant), etc. Mais ces solutions peuvent sans doute être facilement contournées par le FBI et *al.*

Une autre solution serait Safeweb[32], locigiel open-source et gratuit d'une start-up américaine est à disposition du public depuis février 2001. Il permet de rendre impossible l'identification de la source et de la destination d'une information interceptée sur les réseaux IP. Mais une solution pour passer outre cet anonymat sera sans doute ou a déjà été trouvée par la NSA dans la mesure où le plus gros client de Safeweb est la CIA.

Quelques questions demeurent :

- Le cadre du Conseil de l'Europe, école des droits de l'homme, pour un accord international en matière de cybercriminalité n'a t-il pas été choisi pour faire accepter plus facilement un projet attentatoire aux droits de l'homme ? D'autant plus que le système européen est non contraignant, tant au niveau des règles relatives à l'adoption des décisions, qu'au niveau du respect par les parties à la Convention de leurs obligations.[33] Par exemple les Etats non membres du Conseil de l'Europe, partie à la Convention ne sont pas soumis à la juridiction du juge européen.

[31] Ian Brown, expert en sécurité Internet à l'University College London, et Brian Gladman, ancien expert en sécurité de l'information du ministère de la Défense britannique.
[32] http://www.safeweb.com
[33] Intervention du Professeur Jean-Jacques Lavenue, le 22 mai 2001 dans le cadre du séminaire Droit international et cyberespace; ordre public interne et ordre public international.

- La participation américaine à un projet développé au sein d'une instance européenne des droits de l'homme n'avait elle pas pour but la mise en place à l'échelle mondiale de système de surveillance de type Carnivore?

- Un Carnivore des Carnivores existe-t-il ?

De nombreuses lois ont donc été prises depuis 2 ans dans de nombreux pays autorisant la surveillance électronique par le biais de clones de Carnivore. Ces lois adoptées sous influence américaine imposent aux FAI une collaboration avec la police nationale et sans doute une mise en place de clones de Carnivore. Le problème est donc celui d'une atteinte à la vie privée (voir infra) mais également un problème économique dans la mesure où les lois prévoient la plupart du temps que les FAI mettent en place ces « Carnivores » à leurs frais.

La théorie du territoire-limite de Michoud et Duguit considère le territoire de la *limite* du pouvoir de l'Etat. Ainsi si les Etats peuvent utiliser des logiciels de type Carnivore sur leur territoire dans le respect de certaines règles, ils ne devraient pas pouvoir utiliser des systèmes de types échelon qui permettent l'espionnage hors du territoire national.

B / La surveillance à l'extérieur du territoire national

1/ La validité de l'accord UKUSA au regard des règles de droit international public

a) la qualification des valeurs dont il est porté atteinte

Traditionnellement, les spécialistes du droit international considèrent qu'un traité, pour être valable, doit avoir été conclu par des sujets capables, selon une volonté libre (c'est-à-dire dépourvue de vices) et doit comporter un objet licite.

Si les deux premières conditions semblent avoir été remplies lorsque la GB et les USA ont conclu l'accord, en revanche, son objet même peut nous faire douter de sa validité.

En effet, si par nature, le domaine de l'espionnage est illégal, secret et, le plus souvent unilatéral (en ce sens qu'il ne concerne généralement qu'un seul Etat), que penser d'un accord international dont l'objet porte sur l'interception généralisée des communications de toute nature ?

Toutefois, il faut bien avouer que dire que la validité d'un traité dépend de la licéité de son objet nécessite d'abord de démontrer qu'il existe un ordre public international.

Avant l'adoption de la Convention de Vienne de 1969, la doctrine se plaçait traditionnellement sur le terrain de la « moralité internationale » ou sur celui de la recherche de normes coutumières supérieures.

- Traités et moralité internationale

Selon le professeur Nguyen Quoc Dinh[34] , « *aucun droit ne peut tolérer l'immoralité, mais le droit ne peut se confondre avec la morale. On ne peut envisager de sanctionner les traités immoraux que si le droit positif est susceptible de recevoir, par un processus de formation spontanée, des règles morales (il s 'agit du concept de droit « objectif », selon les doctrines de Duguit et de G. Scelle). Seul ce droit objectif pourrait servir de fondement positif à un ordre public international auquel le contenu des traités devrait obligatoirement se soumettre* ».

Parmi les exemples de traité contraire aux bonnes mœurs (qui sont, il est vrai, assez rares), nous pouvons notamment relever l'affaire « Etats-Unis contre Krupp », dans laquelle un tribunal militaire international de l'après-guerre a affirmé : « *Nous n'avons aucune hésitation à conclure que si Laval ou l'ambassadeur de Vichy à Berlin a conclu un accord quelconque sur l'emploi des prisonniers de guerre français dans l'industrie allemande, un tel accord aurait été manifestement contraire aux bonnes mœurs et, partant, nul* ».

- Traités et normes coutumières supérieures

Il s'agit en l'espèce, essentiellement de la théorie développée par le professeur Scelle selon laquelle un traité ne saurait déroger à une coutume solidement établie.
Selon lui, il convient de reconnaître, au sein du droit coutumier, l'existence d'une hiérarchie entre les normes impératives, d'une part, (jus cogens) et celles modifiables par une convention postérieure, d'autre part, (jus dispositivum).

Le contenu même de ces normes est évidemment flou, il dépend du contexte spatio-temporel au cours duquel il est étudié.

Sachant qu'une règle de jus cogens est une norme «acceptée et reconnue comme telle par la communauté internationale des Etats dans son ensemble, nous pouvons donc essayer d'intégrer les libertés individuelles et le secret des communications dans ce type de norme (il faut bien insister sur le terme « essayer » car évidemment, il existe des divergences doctrinales).

Cette opinion peut, par ailleurs, être confortée par le professeur Nguyen Quoc Dinh, selon lequel, « *le domaine de cette « super-légalité internationale », de ce que G. Scelle appelle « le droit commun international », est défini par des critères matériels : normes garantissant les libertés individuelles, telles : le droit à la vie qui va à l'encontre de la guerre, la liberté corporelle qui s'oppose à l'esclavage, la liberté de circulation, du commerce et d'établissement qui est incompatible avec la fermeture abusive des frontières (…). Recourir à des critères matériels est supposer résolu le problème des modalités de formation de l'ordre public international dans une société peu intégrée* ».

Nous en arrivons donc à la Convention de Vienne de 1969, laquelle consacre la primauté des normes de jus cogens.

Ainsi, aux termes de l'article 53 de cette convention, «*Est nul tout traité qui, au moment de sa conclusion, est en conflit avec une norme impérative du droit international général. Aux*

[34] Nguyen Quoc Dinh, Droit International Public, LGDJ, 6ème édition

fins de la présente convention, une norme impérative du droit international général est une norme acceptée et reconnue par la communauté internationale des Etats dans son ensemble, en tant que norme à laquelle aucune dérogation n'est permise et qui ne peut être modifiée que par une nouvelle norme du droit international général ayant le même caractère ».

Cet article 53 est complété par un article 64 qui précise que « *si une nouvelle norme impérative du droit international général survient, tout traité existant qui est en conflit avec cette norme devient nul et prend fin* ».

Au-delà des discussions doctrinales , nous pouvons donc envisager que le respect des libertés des citoyens des différents Etats constitue une règle de jus cogens dont la violation systématique doit être sanctionnée.

Partant du postulat qu'aucun Etat partie à ce traité ne désire soulever son éventuelle nullité, la véritable question qui se pose est alors de savoir si des Etats non partie peuvent le faire.

Il faut donc s'interroger sur le caractère de la nullité de ce traité et sur les parties susceptibles d'en réclamer l'annulation.

b) la question de l'éventualité d'un recours

Tout le monde connaît la distinction, en droit interne, entre nullité absolue et nullité relative, en fonction de la gravité de l'illégalité (il s'agit généralement de savoir si l'illégalité affecte l'intérêt général et trouble l'ordre public). En matière de droit international, certains auteurs excluaient totalement, toute idée de nullité absolue. Ce débat doctrinal n'a plus de sens depuis l'adoption de la convention de Vienne qui a retenu cumulativement ces deux types de nullité.

Ainsi, l'article 53 sur les traités en conflit avec le jus cogens prévoit une sanction forte (la nullité de l'accord) dans le but de défendre l'ordre public international. Par ailleurs, le caractère absolu de cette nullité découle également directement de l'article 45 de la Convention qui l'écarte du champ d'application de
De plus, l'article 45 de la Convention qui prévoit la règle de la confirmation expresse ou tacite des actes nuls écarte expressément

Il faut toutefois se demander si la notion de nullité absolue au sens de la Convention coï ncide entièrement avec la même notion que le droit interne. En effet, selon ce dernier, toute personne intéressée, contractante ou non, peut se prévaloir d'une nullité absolue. Or, selon le professeur Nguyen Quoc Dinh, si les textes des articles 51, 52 et 53 utilisent des formules impersonnelles qui n'interdisent pas explicitement une telle interprétation, celle-ci semble être contredite par les articles 65 et 66 qui n'ouvrent l'action en nullité qu'aux seules parties.

A bien y réfléchir, cela peut sembler choquant. Il serait quand même préférable de considérer qu'en cas de violation d'une règle de jus cogens tout Etat pourrait demander la nullité du traité en question.

C'est ce qui semble avoir été admis par la C.I.J. dans un obiter dictum de l'arrêt du 5 février 1970, (affaire de la Barcelona Traction) : « *une distinction essentielle doit (…) être établie entre les obligations des Etats envers la communauté internationale dans son ensemble et celles qui naissent vis-à-vis d'un autre Etat dans le cadre de la protection diplomatique. Par leur nature même, les premières concernent tous les Etats. Vu l'importance des droits en cause, tous les Etats peuvent être considérés comme ayant un intérêt juridique à ce que ces droits soient protégés ; les obligations dont il s'agit sont des obligations « erga omnes ».*
La Cour a ensuite poursuivi en annonçant la possibilité d'une « actio popularis » lorsque les normes violées sont des normes de jus cogens.

Si l'on admet ce raisonnement et que l'on envisage l'hypothèse d'un recours possible des Etats non-partie, les moyens de règlement possibles de ce différend doivent être exposés.

Ainsi, pourront éventuellement être utilisées, les dispositions de l'article 33 de la charte des NU (art.65 de la Convention de Vienne) qui prévoient plusieurs moyens de règlement pacifique des litiges, ou encore, celles de l'article 66 de ladite Convention, lesquelles prévoient notamment qu'en cas de nullité provenant d'un conflit entre le traité et les normes de jus cogens les parties peuvent décider d'un commun accord de soumettre leur différend à l'arbitrage.

L'article 66a poursuit en énonçant que « sinon, toute partie à ce différend, par une requête unilatérale, peut porter l'affaire devant la Cour Internationale de Justice, dont la compétence est, dans ce cas, obligatoire ».

En ce qui concerne les effets de cette nullité, si elle était un jour constatée, il faut préciser que bien que le principe soit la nullité ab initio, c'est-à-dire, que le traité est considéré comme nul depuis le jour de sa conclusion, et non pas seulement à partir du moment de la découverte de sa nullité (la nullité est donc comme en droit commun, rétroactive, art.69 {1 de la Convention), il faut bien avouer que cela n'aurait aucun sens en ce qui nous concerne.

Ainsi, l'article 71 précise que si la nullité découle de la violation d'une norme de jus cogens, la conséquence de la nullité consiste moins dans un ajustement des rapports entre les parties que dans l'obligation pour chacune d'elles de mettre sa propre situation en concordance avec cette norme.

Il faut toutefois constater que toutes ces dispositions ne s'adressent qu'à des parties aux traités et n'envisagent pas l'hypothèse d'un recours d'un Etat tiers.

Ainsi, non content de porter une atteinte surdimensionnée à la souveraineté des Etats « écoutés », nous pouvons donc voir que la possibilité d'un recours de ces Etats contre le pacte, en plus d'alimenter une grande discussion doctrinale, soulève des questions quant à sa mise en œuvre.

Cependant, la mise en place d'Echelon et, plus généralement de la conclusion de l'accord UKUSA pouvait se justifier, tout au moins, au départ, ce que nous traiterons dans une prochaine partie.

Avant cela, il faut bien se rendre compte que le système Echelon utilise une technologie très poussée , les moyens techniques mis en œuvre doivent donc être présentés.

2/ Les moyens techniques mis en œuvre

a) Echelon, un outil au service de la NSA

La NSA (National Security Agency), l'organisation qui est chargée de l'interception des communications de toutes sortes, est beaucoup plus riche que la CIA. On estime qu'elle emploie au moins 100 000 personnes dans le monde et dispose d'un budget réel que certains évaluent à plus de 16 milliards de dollars (soit près de 100 milliards de francs).

Selon John Pike, un spécialiste des questions de renseignement à la Fédération des Scientifiques américains, «*aujourd'hui la gigantesque NSA capte tout ou presque* (…), *95% des communications passent dans ses ordinateurs géants. Oui, la quasi- totalité des conversations téléphoniques, des fax, des e-mails et des transferts informatiques est interceptée* ».

Il convient toutefois de souligner que tout le monde n'est pas d'accord avec cette évaluation maximale. Mais il est clair que le pourcentage est très élevé. Dans l'une de ses rares interviews, le patron de la NSA reconnaissait que l'agence devait traiter autant d'informations qu'il y en a dans la Bibliothèque du Congrès (sachant que c'est la plus grande du monde) et ce... toutes les trois heures.

b) l'interception des ondes radio, téléphoniques et des communications Internet

Ce flux prodigieux est alimenté d'abord par des bases secrètes qui « écoutent » les satellites de communication (essentiellement les Intelsat). L'Amérique dispose d'une cinquantaine de stations de ce type dans une vingtaine de pays disséminés sur les cinq continents. Les plus importantes sont en Angleterre, en Nouvelle- Zélande, au Japon, en Allemagne et en Australie à Pine Gap.

Ces bases sont d'une efficacité redoutable. Elles « espionnent » les satellites de communication de deux façons : soit elles interceptent directement le faisceau lorsqu'il descend sur terre ; soit elles se placent près des satellites de communication et détournent leur trafic. Ces « espions de l'espace » tels que Mercury, Mentor ou Trumpet guettent aussi les émissions radioélectriques en provenance de la Terre. Grâce à leurs immenses antennes (de la taille d'un terrain de football), ils captent par exemple les ondes émises par les stations-relais des téléphones mobiles...

Il y aurait neuf satellites ultrasecrets de ce type en orbite géostationnaire, dont deux au-dessus de l'Europe. Ces derniers envoient leurs informations vers l'immense base de la NSA de Menwith Hill, en Grande-Bretagne.

Selon certains spécialistes, chaque fois que l'on téléphone à l'étranger et que l'on entend un écho (c'est un signe que c'est un satellite et non un câble qui relaie la communication), cette discussion est « traitée » par la NSA via ses stations au sol.

En ce qui concerne les communications transatlantiques qui passent par des câbles sous-marins les communications ne sont pas plus à l'abri des écoutes. Ainsi, il y a quelques années, il s'agissait de câbles téléphoniques traditionnels. Pour les écouter, un sous-marin de la NSA

installait une « bretelle » à 5 000 mètres sous l'eau. Les spécialistes disent que c'était techniquement lourd mais scientifiquement simple.

Aujourd'hui, les câbles ont disparu et ont laissé place à des fibres optiques sur lesquelles les méthodes d'antan n'ont aucun effet. Elles ne sont pas pour autant « inécoutables ». Certains ingénieurs des télécommunications considèrent ainsi que la NSA aurait inventé un système pour intercepter les transferts de données sous l'eau à un point précis du câble où s'opère l'« accélération » de la communication. Pour d'autres, l'agence est tout simplement en cheville avec les compagnies de téléphone et intervient dans les stations-relais, à la sortie du câble de l'océan.

Il ne s'agit ni de science-fiction, ni de paranoï a, de tels accords secrets avec des sociétés privées ne seraient pas, loin s'en faut, les premiers. Ainsi, dans les années 50 et 60, la NSA, dont à l'époque personne ne soupçonnait l'existence, avait mis au point l'opération Shamrock : les compagnies de télégraphe, la Western Union en particulier, remettaient tous les soirs à un officier de l'agence une copie de l'ensemble du trafic qui entrait aux Etats-Unis ou en sortait.

Au total, la NSA intercepte donc chaque jour des millions de communications de toutes sortes. Elles sont numérisées et envoyées par câble protégé et par satellite à Fort Meade. Là, toutes ne sont pas « enregistrées », loin s'en faut. Seule une petite partie est conservée et traitée.

Le tri peut se faire par numéro de téléphone: ainsi, certains sont systématiquement surveillés (les ambassades importantes, les palais présidentiels, les ministères de pays sensibles...), d'autres le sont selon les circonstances (grandes entreprises, hôtels, conférences internationales...).

On peut aussi sélectionner par reconnaissance vocale : les ordinateurs de l'agence (des Cray dont les puces sont fabriquées dans une usine spéciale à Fort Meade) sont capables d'identifier automatiquement des milliers de personnes par leur voix : des terroristes, des hommes politiques, des diplomates...

Enfin les « clients » de la NSA (la CIA, les Départements d'Etat, de la Défense ou du Commerce) établissent une liste de mots-clés ou d'expressions dont l'apparition dans une conversation, dans un fichier ou un e-mail doit déclencher automatiquement l'enregistrement de la communication. La NSA serait même capable de traduire instantanément des conversations dans plus de cent langues.

Les experts s'accordent également pour dire que sur toutes les communications interceptées, 10 000 à 15 000 sont résumées et font l'objet d'un rapport.

En ce qui concerne Internet, la NSA s'y intéresse évidemment beaucoup.
Selon un ancien de l'agence devenu expert en sécurité informatique, Wayne Madsen, « il est évident que des fournisseurs américains d'Internet autorisent la NSA à "renifler" tout ce qui passe sur le Web et à "filtrer" ce qui l'intéresse ». De même, beaucoup soupçonnent l'agence de piéger des sites Internet (avec ou non la complicité de ces derniers) dans le but de consulter à distance et incognito le contenu des ordinateurs de tous ceux qui se connectent sur le site en question.

Pour certains spécialistes, dans le cas des communications qui ne peuvent être interceptées qu'à proximité de la cible (ce sont principalement celles qui utilisent des ondes courtes), la NSA et la CIA ont créé ensemble une unité d'élite ultrasecrète : le Special Collection Service (SCS). Sous couverture diplomatique, ces spécialistes montent de toutes pièces un service d'écoutes dans les ambassades ou les consulats américains. Parfois ce sont les alliés du Commonwealth - moins suspectés d'espionnage - qui réalisent l'opération, ainsi que le raconte un ancien des services canadiens, Mike Frost.

L'Amérique veut donc tout écouter, tout lire mais aussi tout voir.

c) Echelon et les satellites espions

De très puissants satellites espions « voleurs » d'images sont mis au point par le National Reconnaissance Office (le NRO, créé en 1961 mais dont l'existence a été officiellement niée jusqu'en 1992). Leur précision est impressionnante. A plusieurs centaines de kilomètres, certaines caméras peuvent discerner des objets d'à peine 10 centimètres.

D'autres satellites, les Lacrosse dotés d'un radar, « voient » à travers la nuit ou les nuages avec une précision à peine inférieure. Grâce à leur capteur à infrarouge, d'autres encore sont si sensibles à la chaleur qu'ils relèvent une augmentation d'un dixième de degré au sol : en mesurant les différences de température, ils sont capables de repérer certaines cibles enterrées ou camouflées. Enfin les derniers-nés (KH 12 Improved Crystal) sont apparemment dotés de tous ces différents capteurs.

S'il est vrai que les différentes techniques d'écoutes mises en place sont impressionnantes, il faut maintenant voir quelles sont leur finalité.

3/ Les justifications et les applications du système

Dans un premier temps, lorsque le système a été conçu, il s'agissait de surveiller les Etats du bloc soviétique. Toutefois, après la chute de cet adversaire, les agences de défense et de renseignement se sont réorientées vers de nouvelles missions et, pour justifier leurs budgets, ont effectué des transferts de technologies vers certaines applications à visée répressive, telles les opérations de lutte contre la drogue, le terrorisme ou contre les différents trafics d'armes.

a) la lutte contre le terrorisme et les trafics d'armes

Pour ce qui est du terrorisme, par exemple ; en 1986, deux soldats américains étaient tués dans l'explosion d'une discothèque à Berlin-Ouest. L'attentat n'a pas été revendiqué. Pourtant l'Etat commanditaire, la Libye, a été immédiatement identifié par les Etats-Unis : la NSA avait intercepté et décrypté les communications entre les ambassades de Tripoli à Berlin-Est et Rome. Quelques minutes après l'explosion, un membre des services secrets de Kadhafi disait : « *L'opération a bien eu lieu. Elle n'a pas laissé de traces* ». Quelques jours après, le Président Reagan autorisait le bombardement de la capitale libyenne.

De même, certains évoquent la possibilité que Washington ait communiqué à Paris, le contenu de messages cryptés entre Téhéran et l'ambassade iranienne en France, permettant ainsi à la DST d'identifier avec certitude les meurtriers de l'ancien Premier ministre Chapour Bakhtiar.

Par ailleurs, la lutte contre la prolifération des armes de destruction massive et autres trafics d'armes, constitue également une des justifications invoquées pour justifier de l'existence du système.

C'est notamment la mission des satellites espions. En combinant différents types d'image (radar, infrarouge...), les photo-interprètes savent repérer, dans certains cas, une fabrication cachée de produits chimiques ou bactériologiques.

La NSA, quant à elle, traque les trafiquants de « précurseurs » (les produits de base de ce type d'arme) et les fournisseurs clandestins de technologie militaire. Elle soupçonne (et donc surveille) ainsi, les entreprises russes ou chinoises qui aident l'Iran ou la Corée du Nord dans leurs programmes de missiles balistiques.

Il existe également d'autres champs d'action « honorables »,tels que le suivi des conflits.

b) l'utilisation du système Echelon dans la gestion des conflits internationaux et dans les relations diplomatiques

En juillet 1990, les satellites Keyhole ont vu le déploiement des troupes irakiennes à la frontière du Koweï t. Le 27, soit, six jours avant l'invasion, les capteurs infrarouges ont même repéré les camions militaires transportant de l'eau, du gasoil et des munitions.

De même, selon le « New York Times », la NSA a récemment envoyé des dizaines d'agents au Kosovo pour surveiller le retrait des troupes serbes (et connaître leurs intentions réelles).

Toutefois, il est évident que tout l'arsenal technologique du monde ne remplace pas la décision politique et que d'autres intérêts entrent en jeu: ainsi, en juillet 1995, les Keyhole ont vu les massacres de Srebrenica, mais la Maison-Blanche n'a pas bougé.

Enfin, selon certaines personnes, le système Echelon est également utilisé par Washington comme moyen de pression, par exemple, dans les négociations d'accord de paix.

Ainsi, dans le cadre du conflit israelo-palestinien, la NSA et la CIA peuvent mettre à disposition des parties des photos satellite (par exemple, celles des camps d'entraînement du Hamas), voire, des écoutes de terroristes palestiniens.

Ce rôle des services de renseignement, en général, et du système Echelon, en particulier, dans le cadre des activités diplomatiques est croissant.

Il existe toutefois un aspect « plus obscur» de l'utilisation d'Echelon qui embarrasse les Etats signataires de ce pacte : il s'agit de l'écoute (et donc de l'espionnage) des pays alliés aux USA, tels que, notamment, la France et les autres Etats membres de l'Union Européenne.

c) le problème de l'espionnage des pays « alliés »

Face à cela, les Etats membres du système Echelon (USA en tête) essaient de justifier cette pratique par un comportement commercial déloyal de la part de « leurs amis » et invoquent une finalité « louable » : celle de la lutte contre la corruption internationale.

Ainsi, selon eux, il n'est pas question d'espionner au profit de sociétés américaines car «cela nuirait à la libre concurrence ».

Toutefois, les services secrets peuvent aider les compagnies américaines dans un cas : pour dénoncer les pots-de-vin qui permettent à des firmes étrangères d'obtenir des gros contrats aux dépens de firmes américaines.

C'est ce qui s'est passé en 1995, à propos de Thomson qui devait remporter le marché de la couverture radar de l'Amazonie, mais, au dernier moment, la NSA aurait informé la Maison-Blanche du montant des dessous-de-table versés par l'entreprise française à des responsables brésiliens, et Bill Clinton serait personnellement intervenu auprès de Brasilia pour retourner la situation. En définitive, c'est la société Raytheon qui a obtenu le contrat.

De même, Airbus aurait perdu une grosse vente dans le golfe Persique au profit de Boeing pour des raisons similaires.

A présenter le système Echelon comme cela, on pourrait se dire qu'il est impossible d'y échapper, de «passer entre les mailles du filet ». Or, il n'en est rien, le manque de personnel et le développement des moyens de cryptologie montrent les limites du système.

d) un système qui n'est pas infaillible

Ce système n'avait prévu ni les attentats en Afrique contre les ambassades américaines, ni le tir d'un missile balistique par la Corée du Nord au-dessus du Japon et surtout, les membres du pacte UKUSA, n'avaient pas anticipé les essais nucléaires en Inde au mois de mai alors que les nombreuses photos aériennes qui avaient été prises pouvaient facilement le laisser prévoir.

Ainsi, pour bien comprendre la masse incroyable de documents à traiter, il faut s'imaginer un bloc de papier de 2 mètres de large, 2 mètres de haut et 20 mètres de long qui passe sur un tapis roulant toutes les dix minutes et cela, chaque jour.
Par ailleurs, la NSA détruit chaque année, dans un bain spécial, plus de 1 000 tonnes de documents inutilisés.

Un autre aspect des limites du système réside dans la cryptologie.

Ainsi, alors que, dans les années 60, les machines à coder les communications étaient rares, extrêmement chères (et souvent la NSA avait passé un accord secret avec le fournisseur pour qu'il lui en livre les clés (comme ce fut le cas avec la compagnie suisse Crypto AG)), aujourd'hui, ces techniques se sont développées et démocratisées.

N'importe quel marchand de matériel téléphonique propose des brouilleurs et des codeurs à des prix très bas. » La plupart peuvent être « cassés » facilement par la NSA. Mais pas tous :

certains possèdent des clés très longues ; les découvrir nécessite des jours, des mois, voire plus de traitement informatique et entre-temps, l'information recherchée est devenue périmée.

La NSA a donc demandé à l'administration Clinton de contraindre les fabricants de matériel de cryptographie de rendre leur matériel « écoutable » par l'agence. Après une dure bataille au Congrès, la Maison-Blanche a dû faire machine arrière. De même, l'OCDE a refusé, de rendre obligatoire ce type de garde-fou pour les équipements informatiques, malgré, là encore, la pression de Washington, mais aussi de Londres et de Paris.

Après l'exposé de certaines applications du système Echelon et des moyens techniques mis en œuvre, certains évoquent un risque possible de cyberguerre.

4/ Le risque annoncé d'une cyberguerre

A mon sens, même s'il peut contribuer à intensifier les effets ou faciliter sa mise en œuvre, la cyberguerre a déjà commencé (il faudrait plutôt parler de cyber-guerrilla, bien localisé) mais sans nécessairement utiliser le système en question.

Sur ce point, je pense qu'Internet est beaucoup plus dangereux que le système Echelon lui-même. Je prendrai pour exemple, l'attaque du site de la maison blanche et d'autres sites institutionnels américains par des hackers chinois[35]. Dans cet article, nous pouvions ainsi lire que « L'Amérique est la cible depuis plusieurs jours d'attaques massives de la part de pirates informatiques Chinois. Lundi, c'est le site internet de la Maison Blanche qui était bombardé d'e-mails ainsi qu'une vingtaine d'autres sites américains. Comme celui du département du Travail inaccessible durant quelques jours samedi dernier et dont la page daccueil représentait la photo du pilote chinois disparu à la suite de la collision de son chasseur avec un avion espion américain, le 1er avril dernier au large de l'île de Hainan. On pouvait y lire: "Le pays entier regrette la perte irrémédiable du meilleur de ses fils - Wang Wei, tu vas nous manquer jusqu'à la fin des jours". Le site du département de la Santé health. gov avait également été piraté par une photo du Chinois en uniforme.
Selon la société américaine iDefense, il s'agit d'une opération de grande envergure lancée contre des sites commerciaux et gouvernementaux américains.
Un groupe de pirates informatiques chinois tenait même dimanche une "réunion de mobilisation en réseau" afin d'établir une campagne d'attaques d'une durée d'une semaine contre les sites d'entreprises américaines et les réseaux informatiques yankee. Il faut dire aussi que des pirates pro-américains avaient récemment attaqué 23 sites chinois dans la même journée, et notamment celui du site du Quotidien de la Jeunesse de Pékin.

"Red Guest" est le nom donné à cette cyber-guerre qui devrait durer jusqu'au 7 mai, date anniversaire du bombardement, en 1999, de l'ambassade de Chine à Belgrade par un avion américain. Parmi les menaces de frappes envisagées: le postage d'e-mails comportant des virus à des fonctionnaires américains ainsi que l'envoi massif de données diverses pour surcharger les réseaux et paralyser de nombreux sites (…) ».

[35] « les hackers chinois attaquent l'Amérique », www.linternaute.com, 02.05.01

A mon sens, cet article illustre bien le fait que les systèmes d'interception des communications, en général, et le système Echelon, en particulier, même si, de par leur fonction, peuvent aider à prendre des mesures qui entrent dans le cadre d'une cyberguerre, pour autant, ils n'en sont pas les instruments les plus dangereux.

(En définitive, si une cyberguerre s'entend comme étant la possibilité de bloquer les communications d'un Etat à distance, Internet est une arme beaucoup plus dangereuse).

II / Quelles limites à la surveillance globale à l'international et en interne ?

Comme nous l'avons vu la surveillance des flux d'informations existe depuis longtemps, elle s'exerce aussi bien sur le territoire national que de manière transfrontière, la collecte des informations est instantanée et continue. Par ailleurs, d'abord motivée par des nécessités militaires, elle s'oriente depuis les années 1980 vers la sphère économique[36]. Un dernier constat, semble être que cette pratique tend à ce développer tout autour de la planète[37] et que les outils mis à sa disposition sont de plus en plus efficaces.

Certes la surveillance des flux d'informations peut se justifier au regard des dangers incarnés par le terrorisme, les narcotrafiquants ou encore une éventuelle guerre électronique. La protection de l'ordre public interne et de la sécurité nationale oblige l'Etat à s'adapter aux avancées technologiques et ainsi à pratiquer les interceptions. Il ne s'agit que de la prise en compte des changements induits par l'émergence de la « société de l'information ».

Lorsque la surveillance est pratiquée par l'Etat sur son propre territoire, il n'exerce que des compétences légitimes dans le cadre de l'exercice de sa souveraineté nationale, sous réserve de respecter des objectifs définit par l'ordre public interne et une certaine procédure. Nous verrons toutefois, que les libertés individuelles des citoyens sont sérieusement fragilisées par la mise en œuvre d'une surveillance globale à l'échelle nationale. Ainsi, le renforcement de garde fous et l'établissement d'un débat national s'imposent.

S'agissant de la mise en place d'une surveillance globale orientée vers l'extérieur de l'Etat, elle peut se justifier sous couvert de la protection de la sécurité nationale et par le fait qu'elle est nécessaire au regard de la mondialisation et des évolutions technologiques. On peut citer pour exemple les objectifs définis par la Belgique dans le cadre de sa loi organique du 30 novembre 1998 relatifs aux services de renseignements : « rechercher, analyser et traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique et économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel. »[38]

---

[36] *Réseau Echelon : la justice française ouvre une enquête ;* Philippe COUVE ; http://www.fas.org/irp/program/process/echelon.htm

[37] *Comment la NSA espionne le monde ;* Confidentiel - Défense - juillet 2000 - http://www.confidentiel-defense.com

[38] article 7

Toutefois, cette surveillance s'effectue au mépris de la souveraineté des autres Etats et des droits de leurs citoyens. D'une part, car elle ne s'exerce pas dans le cadre de la protection d'un ordre public international encore à définir et d'autre part, parce que son utilisation dépasse largement la simple défense de la sécurité nationale de ceux qui la pratiquent.

A / Les atteintes aux droits des autres Etats

Echelon et tous les systèmes œuvrant à la surveillance globale du monde mettent en lumière deux questions majeures au regard du droit des Etats, donc du droit international public.

La première, rappelle quelques similitudes avec celle posée par Internet : quelles sont les incidences du caractère transfrontière, instantané et continu des interceptions sur la compétence et la souveraineté des Etats et sur le droit international public ? (1)

La seconde, est plus géopolitique que juridique : quel est l'impact d'Echelon sur les alliances économiques et militaires internationales ? Ou d'une façon un peu moins naïve : que nous révèle Echelon sur l'état des alliances économiques et militaires internationales ? (2)

1 / L'Etat et le droit international confronté à la suppression des frontières et à l'instantanéité en matière d'interception

Comme nous l'avons vu, « l'espionnage » est par essence illégal, il implique de fait de transgresser la loi, c'est ce qui impose en partie le plus grand secret. L'interception internationale des signaux et communications s'effectue en dehors des lois, et échappe à la plupart des juridictions nationales. Cette illégalité réside dans le non respect des normes internationales et de la souveraineté des Etats.

Ce constat n'est pas nouveau, l'espionnage n'est pas né avec Echelon, par contre ce qui est né avec Echelon c'est le caractère continu de la violation de ces droits. La souveraineté des Etats est sapée chaque jour, de façon continue et instantanée. De plus ces interceptions ne sont pas localisables et se font en tout point du globe, sans que l'Etat puisse avoir un contrôle des flux transitant sur son territoire, d'où l'impossibilité de se raccrocher aux frontières et à l'espace qu'elles sont censées protéger et définir.

a) Des interceptions continues et transfrontières en violation des accords internationaux …

Duncan Campbell relate dans son livre une anecdote révélatrice de l'état d'esprit dans lequel se déroule SIGINT et COMINT : « durant les années 80, le personnel et les visiteurs qui pénétraient le Building 600, le bloc d'opération de la RAF[39] Chicksand – base d'écoute U.S. Air Force en Angleterre – passaient un tourniquet et présentaient leur badge de sécurité pour se retrouver nez à nez avec une plaisanterie interne à SIGINT. Une copie de la Convention des Télécommunications Internationales était collée au mur. La Convention, que les Etats-Unis et l'Angleterre avaient tout deux ratifiée, promettait que les Etats membres protégeraient

[39] Royal Air Force

la confidentialité des communications. En passant, les opérateurs se préparaient à faire le contraire »[40].

Cette anecdote souligne que les Etats membres du réseau Echelon pratiquent les interceptions en toute connaissance de cause. La signature des accords internationaux étant reléguée à une simple déclaration de bonnes intentions, qui en pratique n'est pas respectée. Cette idée est renforcée par l'impunité dont jouissent les Etats qui se rendent coupables de telles pratiques.

Ainsi, nous verrons que même si le droit international encadre ces pratiques au travers d'accord multilatéraux, il n'en demeure pas moins que la surveillance et l'interception des communications se pratique à l'échelle mondiale et qu'il s'agit d'un phénomène incoercible.

- **La Convention des Télécommunications Internationales du 2 octobre 1947[41] :**

L'objet de cette Convention est de régir les communications internationales. Elle dispose dans son article 22 que tous les Etats membres s'engagent à assurer la confidentialité de la correspondance internationale[42]. Echelon est là pour nous démontrer que cet engagement est resté lettre morte.

Toutefois, l'alinéa 2 de l'article 22, prévoit des possibilités d'interceptions : « Ils (les Etats membres) se réservent néanmoins le droit de communiquer ces entretiens aux autorités compétentes en vue de garantir l'application des législations nationales ou l'exécution des conventions internationales auxquelles ils sont parties. »

On pourrait ainsi penser que UKUSA, entre dans le cadre « des conventions internationales auxquelles ils sont parties ». Mais il n'en ait rien, comme nous l'avons vu, l'accord UKUSA n'entre pas dans le cadre de ce que l'on pourrait définir comme une convention internationale au sens de « loi internationale ».

En effet, l'article 22 ne semble viser que ce que l'on nomme comme étant un «traité loi » ou « traité normatif »[43], dont l'objet est d'établir une situation juridique impersonnelle et objective. Alors que UKUSA n'apparaît que comme un « traité contrat », générateur de situations juridiques subjectives, les contractants stipulant des prestations réciproques. De plus, l'article 22 n'envisage que des objectifs de maintien de l'ordre, ce qui ne correspond qu'en partie aux objectifs d'Echelon.

Il nous semble important de souligner que la Convention des Télécommunications Internationales est à l'origine de la création de l'Union Internationale des Télécommunications[44] qui est basée à Genève. l'UIT est devenue une agence spécialisée du système des Nations Unies en 1947; l'un de ses principaux objectifs est de « Maintenir et

[40] Surveillance Electronique Planétaire, Duncan Campbell, édition ALLIA, p 118 - 119
[41] Texte en anglais de la Convention, http://www.austlii.edu.au/au/other/dfat/treaties/1949/1.html
[42] « Les membres conviennent de prendre toutes les mesures possibles compatibles avec le système de télécommunication utilisé en vue de garantir la confidentialité des communications internationales. »
[43] Lexique des termes juridiques, Raymond Guillien et Jean Vincent, 10éme édition, DALLOZ, p480
[44] UIT / Pour une présentation plus détaillée : http://www.france.diplomatie.fr/frmonde/nuoi/3sysonu/isp/uit.htm & http://www.itu.int

étendre la coopération internationale pour l'amélioration et l'emploi rationnel des télécommunications ; ».

Bien évidemment l'ensemble des Etats participant à Echelon sont membres de l'UIT. Ainsi, dans la perspective d'un débat et d'une collaboration internationale sur le thème des interceptions, l'UIT devrait en toute logique jouer un rôle non négligeable.

- **La Convention de Vienne du 18 avril 1961 sur les relations diplomatiques[45] :**

Cette convention a pour objet d'encadrer les relations diplomatiques et notamment d'établir le statut des diplomates et des ambassades, on se référera à l'article 27 qui dispose :

1. L'état accréditaire permet et protège la libre communication de la mission pour toutes fins officielles. En communiquant avec le gouvernement ainsi qu'avec les autres missions et consulats de l'état accréditant où qu'il se trouve, la mission peut employer tous les moyens de communication appropriés, y compris les courriers diplomatiques et les messages en code ou en chiffre. Toutefois, la mission ne peut installer et utiliser de poste émetteur de radio qu'avec l'assentiment de l'état accréditaire.

2. La correspondance officielle de la mission est inviolable. L'expression "correspondance officielle" s'entend de toute correspondance relative à la mission et à ses fonctions.

Là encore les pays membres de l'UKUSA ont aussi ratifié cette Convention, cependant les échanges diplomatiques constituent une cible privilégiée des interceptions, comme le rappelle Duncan Campbell lors d'une interview accordée à RFI[46]. La raison est simple et évidente, les échanges entre une ambassade et ses correspondants présents sur le territoire étatique sont le plus souvent sensibles.

On peut rappeler les deux exemples cités précédemment[47], s'agissant de l'attentat à la bombe ayant eu lieu en 1986 dans une discothèque de Berlin-Ouest et de l'assassinat de l'ex-premier Ministre Iranien Chapour Bakhtiar.

Ces deux exemples portent sur des interceptions qui étaient motivées par des impératifs de sécurité et de maintien de l'ordre, néanmoins elles sont la preuve que les communications diplomatiques ne sont pas épargnées par SIGINT et COMINT, et que la Convention de Genève n'est pas respectée. On peut supposer à juste titre que ces interceptions sont généralisées et continues. Comme l'avoue lui même le directeur de la NSA : « Il n'y a pas un seul événement de politique étrangère qui n'intéresse le gouvernement américain et auquel la NSA ne soit pas directement mêlée ».

Les Etats-Unis apparaissent alors comme un Etat omniscient, omniprésent voire omnipotent et avec eux les Etats qui sont membres de l'accord UKUSA. On comprend alors que la présence du Royaume-Uni au sein de cette alliance est source de tentions et d'interrogations au sein de l'union Européenne dont elle fait aussi partie.

---

[45] http://www.admin.ch/ch/f/rs/c0_191_01.html

[46] Trois question à Duncan Campbell, http://cdcp.free.fr/dossiers/echelon/dc.htm, *Interview pour Radio France International*

[47] *Comment la NSA espionne le monde ;* Confidentiel - Défense - juillet 2000 - http://www.confidentiel-defense.com

- **Le Traité instituant la Communauté européenne (signé à Rome le 25 mars 1957) & le Traité sur l'Union européenne (signé à Maastricht le 7 février 1992)[48]**

Dans un premier temps, nous envisageront les atteintes au traité instituant la Communauté européenne (traité CE) et au traité sur l'Union européenne (Traité UE) sous un angle assez général, nous traiterons plus tard des atteintes possibles à l'article 286 CE et à l'article 6 UE, qui sont l'objet d'une partie consacrée à la protection des individus et des entreprises.

Dans un second temps nous étudierons la réaction de l'Union européenne en temps qu'entité suite à la « découverte » d'Echelon.

♦ L'atteinte à l'esprit même des textes …

La présence concomitante du Royaume-Uni au sein de l'UE et au sein d'UKUSA peut apparaître à ses partenaires européens comme une déloyauté totale, notamment au regard de l'esprit animant les différents traités européen ratifié par la Grande Bretagne.

En premier lieu, on peut se référer à l'article 3 du traité CE, figurant dans « Les principes » inclus dans la première partie du traité. Cet article dispose à son premier alinéa : « Aux fins énoncées à l'article 2, l'action de la Communauté comporte, dans les conditions et selon les rythmes prévus par le présent traité : g) un régime assurant que la concurrence n'est pas faussée dans le marché intérieur, ».

Au regard de la reconversion de SIGINT et COMINT vers l'espionnage économique, on peut dès à présent établir que le Royaume-Uni viole un des principes fondateurs de la communauté : l'établissement d'une concurrence saine et loyale au sein du marché commun.

Dans ce contexte, on pourra s'émouvoir à la lecture de l'article 154[49], figurant au titre XV relatif aux « Réseaux transeuropéens ». En effet, il prévoit que la Communauté doit faciliter et mettre en place de réseaux transeuropéens notamment dans le secteur des télécommunications. L'alinéa 2 disposant : « la Communauté vise à favoriser l'interconnexion et l'interopérabilité des réseaux nationaux ainsi que l'accès à ces réseaux ». Ainsi, le traité CE ouvre grand la porte et facilite la mise en œuvre de processus SIGINTet COMINT.

---

[48] Texte intégral, http://europa.eu.int/eur-lex/fr/treaties/dat/treaties_fr.pdf

[49] *Article 154* :

1. En vue de contribuer à la réalisation des objectifs visés aux articles 14 et 158 et de permettre aux citoyens de l'Union, aux opé-rateurs économiques, ainsi qu'aux collectivités régionales et locales, de bénéficier pleinement des avantages découlant de la mise en place d'un espace sans frontières intérieures, la Communauté contribue à l'établissement et au développement de réseaux trans-européens dans les secteurs des infrastructures du transport, des télécommunications et de l'énergie.
2. Dans le cadre d'un système de marchés ouverts et concurrentiels, l'action de la Communauté vise à favoriser l'interconnexion et l'interopérabilité des réseaux nationaux ainsi que l'accès à ces réseaux. Elle tient compte en particulier de la nécessité de relier les régions insulaires, enclavées et périphériques aux régions centrales de la Communauté.

S'agissant du traité sur l'Union européenne, on s'arrêtera tout d'abord sur l'article 2[50] qui dispose que l'Union se donne notamment pour objectif la définition et l'établissement d'une politique de défense commune.
Cet objectif semble pour le moins incompatible avec les activités parallèles du Royaume-uni au sein d'Echelon. Surtout au regard des dispositions de l'article 11[51] du traité sur l'Union européenne, traitant de la mise en œuvre d'une politique étrangère et de sécurité couvrant tous les domaines de la politique étrangère et de sécurité.

On pourra légitiment s'interroger sur les facultés de la Grande Bretagne à respecter les principes de solidarité et de loyauté établis à l'alinéa 2 : « Les États membres appuient activement et sans réserve la politique extérieure et de sécurité de l'Union dans un esprit de loyauté et de solidarité mutuelle. Les États membres œuvrent de concert au renforcement et au développement de leur solidarité politique mutuelle. Ils s'abstiennent de toute action contraire aux intérêts de l'Union ou susceptible de nuire à son efficacité en tant que force de cohésion dans les relations internationales ».

Ainsi, la présence du Royaume-Uni au sein d'Echelon heurte de plein fouet les principes et objectifs définis dans le cadre de l'Union européenne. Reviennent alors à nos oreilles les mots du Général de Gaule, qualifiant la Grand Bretagne de Cheval de Troie des Etats Unis.

Peu après la ratification du traité de Nice[52] précisant notamment les objectifs en matière de sécurité commune et le renforcement de la protection à l'égard des données personnelles et des droits des individus, il semble plus que nécessaire que le Royaume Uni clarifie ses alliances et sa politique vis à vis de ses partenaires.

- …n'empêche pas une réaction ambiguë de l'Union

---

[50] *Article 2* : L'Union se donne pour objectifs: d'affirmer son identité sur la scène internationale, notamment par la mise en oeuvre d'une politique étrangère et de sécurité commune, y compris la définition progressive d'une politique de défense commune, qui pourrait conduire à une défense commune, conformément aux dispositions de l'article 17;

[51] *Article 11 :* 1. L'Union définit et met en œuvre une politique étrangère et de sécurité commune couvrant tous les domaines de la politique étrangère et de sécurité, dont les objectifs sont:
— la sauvegarde des valeurs communes, des intérêts fondamentaux, de l'indépendance et de l'intégrité de l'Union, conformément aux principes de la charte des Nations unies;
— le renforcement de la sécurité de l'Union sous toutes ses formes;
— le maintien de la paix et le renforcement de la sécurité internationale, conformément aux principes de la charte des Nations unies, ainsi qu'aux principes de l'acte final de Helsinki et aux objectifs de la charte de Paris, y compris ceux relatifs aux frontières extérieures;
— la promotion de la coopération internationale;
— le développement et le renforcement de la démocratie et de l'État de droit, ainsi que le respect des droits de l'homme et des libertés fondamentales.

[52] JOCE, 10 mars 2001, (2001/C 80/01)

L'alliance UKUSA a été établie par un accord secret de 1947, et il a fallu attendre le 5 juillet 2000[53] pour que l'Union européenne réagisse officiellement en créant une commission temporaire sur le système Echelon. Les objectifs de cette commission sont les suivants :

- vérifier l'existence du système d'interception des communications connu sous le nom d'ECHELON et dont l'activité est décrite dans le rapport STOA sur le développement des technologies de surveillance et le risque d'abus d'informations économiques;
- vérifier la compatibilité d'un tel système avec le droit communautaire, en particulier l'article 286 du traité CE et les directives 95/46/CE et 97/66/CE, et avec l'article 6, paragraphe 2, du traité sur l'Union européenne, sur la base des questions suivantes:
- les droits des citoyens européens sont-ils protégés contre les activités des services secrets ?
- le cryptage constitue-t-il une protection adéquate et suffisante pour protéger la vie privée des citoyens ou faut-il prendre des mesures complémentaires et, dans l'affirmative, de quel ordre ?
- comment renforcer la prise de conscience des institutions européennes à l'égard des risques suscités par ces activités, et quelles mesures peut-on prendre ?
- vérifier si l'interception des communications au niveau mondial fait courir des risques à l'industrie européenne,
- proposer, le cas échéant, des initiatives politiques et législatives;

Outre le caractère naï f de certaines questions, comme « vérifier si l'interception des communications au niveau mondial fait courir des risques à l'industrie européenne », on peut surtout s'étonner qu'il ne s'agisse que d'une commission temporaire et non d'une commission d'enquête.

170 députés avaient bien réclamé la constitution d'une commission d'enquête, mais elle avait été écartée par les présidents de groupes le 13 avril 2000, une seconde tentative avait eu lieu mais le mercredi 5 juillet les eurodéputés ont refusé par 340 voix contre 210 l'idée d'une véritable commission d'enquête[54].

Ce choix semble révéler le malaise qui parcours l'Union européenne, d'une part car le Royaume Uni est directement impliqué et d'autre part car l'Allemagne et la France sont aussi coupables de liaisons dangereuses, participants et mettant en place des systèmes de surveillance globale.

Les trois plus grandes nations de l'UE semblent vouloir à tout pris éviter un débat de fond. Comme semble le confirmer les propos tenus par Alain Krivine, député européen membre de la commission temporaire[55], il explique notamment que les pouvoirs de la commission se limitent à demander des auditions sans pouvoir obliger les personnes à témoigner. L'impossibilité de prendre des mesures contraignantes limite ainsi l'intérêt de cette commission, qui ne semble valoir sa création qu'à la volonté de sauver les apparences.

---

[53] http://www.europarl.eu.int/tempcom/echelon/mandate_fr.htm

[54] L'Europe enquête sur Echelon à reculons, Jean-Marc Manach, http://transfert.net/fr/cyber_societe/article.cfrn?idx_rab=87&idx_art=1141

[55] « je n'attends pas grand-chose des auditions sur Echelon », Alain Krivine porte parole de la LCR et eurodéputé, http://transfert.net/fr/cyber_societe/article.cfrn?idx_rab=87&idx_art=5530

En conclusion, on peut établir que l'esprit de plusieurs traités majeurs est mis à mal par l'existence de s systèmes d'interception globale. Tout comme la règle *Pacta sunt servanda*, et son corollaire qui réside dans l'exécution de bonne foi tel que défini dans l'article 26[56] de la Convention de Vienne. Si l'on se réfère à ce qui est développé par Nguyen Quoc Dinh, Echelon s'inscrit en opposition avec les principes organisant les relation internationales, puisque « le principe de la bonne foi s'élève au rang d'une institution qui régit l'ensemble des relations internationales »[57].

Même si certains Etats de l'Union à commencer par le Royaume-Uni refusent le débat, il n'en demeure pas moins qu'ils ne pourront l'éviter, d'une part car il est amorcé dans la sphère privée, et d'autre part car l'avenir de l'Union, telle qu'elle se dessine dans les traités en dépend.

Mais les ambiguï tés et tentions que suscite Echelon au sein de l'Union européenne ne doivent pas nous faire perdre de vue, le véritable enjeu que représente Echelon. C'est à dire la manifestation de la remise en cause de la conception traditionnelle des compétences et de la souveraineté de l'Etat.

b) … engendrant une remise en cause de la conception traditionnelle des compétences et de la souveraineté des Etats

Echelon, trouve échos dans l'idée avancée par Léo Tindemans dans son Rapport sur l'Union européenne : « l'emprise des gouvernements nationaux sur les leviers qui permettent d'influencer nos sociétés s'est constamment réduite. Sur le plan interne comme sur le plan externe, la marge de manœuvre des États a diminué. Ils cherchent à se maintenir en équilibre face à des données internes et externes qu'ils ne contrôlent pas ».

Cela correspond fidèlement aux rapports qu'entretiennent les Etats et les flux d'informations, ceux-ci ne sont pas en mesure de contrôler ce qui entre sur leur territoire et ce qui en sort. De même ils ne peuvent empêcher l'interception des communications qu'ils émettent et reçoivent, ni leur utilisation par des tiers.

Néanmoins, on pourrait avancer qu'Echelon est un outil afin de rétablir l'équilibre au profit de l'Etat. Ce dernier, ayant la possibilité d'accéder à l'ensemble des informations et d'influer à son avantage au cas par cas. Nonobstant, il ne peut empêcher les flux de circuler ni qu'un autre Etat ne les intercepte, on peut ajouter que plus ce pouvoir est partagé entre un grand nombre d'Etats plus il cesse d'être un avantage décisif. Par ailleurs, l'exercice d'un tel pouvoir n'étant pas reconnu par l'ordre juridique international, l'utilisation des informations doit se faire via des réseaux en marge du droit.

Nous étudierons dans un premier temps, quelles atteintes représente Echelon à l'égard de la notion de souveraineté en temps que manifestation de l'indépendance de l'Etat et à son corollaire incarné par l'égalité souveraine des Etats. Enfin nous essaierons de mesurer les conséquences de l'existence des systèmes de type Echelon sur les compétences des Etats.

[56] « tout traité en vigueur lie les parties et doit être exécuté par elles de bonne foi »
[57] Droit International Public, Nguyen Quoc Dinh, LGDJ, p 216, 6ème édition

- **Atteintes à la souveraineté des Etats et remise en cause du principe d'égalité souveraine**

Au 19ème siècle la souveraineté était généralement défini comme un pouvoir suprême et illimité, Hegel liait la notion de souveraineté à la toute puissance de l'Etat. Mais cette conception absolutiste de la souveraineté n'est plus d'actualité, « ne serait-ce que parce que, dans la société internationale contemporaine, largement inter étatique, la souveraineté de chaque Etat se heurte à celles, concurrentes et égales, de tous les autres Etats … la souveraineté apparaît dans ces conditions, comme la source des compétences que l'Etat tient du droit international »[58].

Le problème est qu'Echelon nous sort de la sphère légale, l'ensemble des activités se fait dans le non respect du droit international, il porte directement atteinte à l'égalité souveraine des Etats, tel que prévue dans la Charte des Nations Unis[59] et ainsi à l'indépendance des Etats donc à leur souveraineté.

En effet, comme il est souligné dans le Rapport d'expertise rédigé à l'attention du Comité Permanent de contrôle des services de renseignements belges[60] « la captation abusive de messages par une personne étrangère remet en cause la souveraineté des Etats en tant qu'expression du principe d'indépendance de chaque Etat dans l'ordre international[61]. Que devient l'indépendance d'un Etat, si les secrets de ses administrations, de son gouvernement, de ses entreprises, de ses citoyens peuvent être décryptés en des lieux inconnus au profit de puissances étrangères du seul fait qu'ils pénètrent l'espace extra atmosphérique ? L'absolue limitation des écoutes est fondamentale pour que survivent l'égalité et l'indépendance des Etats ».

La souveraineté des Etats est compromise suite à la remise en cause de l'ordre juridique international. Cette perte de souveraineté ne s'effectue pas dans le cadre d'un transfert de compétence, dans lequel l'Etat n'est privé que des compétences dont il a accepté le transfert.

---

[58] Droit International Public, Nguyen Quoc Dinh, LGDJ, p 420, 6ème édition

[59] Article 2, paragraphe 1: « l'Organisation est fondée sur le principe de l'égalité souveraine de tous ses membres ».

[60] *Existe-t-il ? Que peut-il faire ? Peut-on et doit-on s'en protéger ?* Rapport d'expertise rédigé à l'attention du Comité Permanent de contrôle des services de renseignements le 7 mars 2000 Par Yves Poullet (yves.poullet@fundp.ac.be) Docteur en Droit Professeur et Directeur du Centre de Recherche Informatique et Droit (FUNDP) & Jean-Marc Dinant (jmdinant@fundp.ac.be) Maître et doctorant en Informatique Chargé de recherche au Centre de Recherche Informatique et Droit de l'Université de Namur

[61] A ce propos, la réflexion de R. de Bottini, Souveraineté et conflits de lois, in La Souveraineté au 20 e siècle, Armand Colin (éd.), 1971, p. 145: « *La raison de cette opposition tient sans doute à l'ambiguï té de la notion de souveraineté, susceptible en l'espèce de recouvrir deux acceptions bien différentes. On peut y voir d'abord le principe d'une délimitation souveraine des compétences législatives de chaque Etat; elle permettrait de fixer unilatéralement dans le domaine spatial les frontières que chaque loi peut avoir par opposition à toutes les autres lois nationales. Mais on peut aussi faire appel à cette notion de souveraineté dans un sens plus banal, selon lequel elle ne serait alors que l'expression du principe d'indépendance de chaque Etat dans l'ordre internationa*l. »

Au contraire, l'altération de sa compétence se fait à son insu et engendre le plus souvent des atteintes à ses propres intérêts et à ceux de ses citoyens.

Le fait que cette technologie soit le monopole de quelques grandes nations, et principalement celui des Etats Unis semble porter un coût décisif au principe d'égalité souveraine des Etats. Certes cette égalité subsiste dans la sphère juridique, l'Etat reste seul maître des traités qu'il signe et ne peut se voire imposer des décision par un autre Etat. Mais, en pratique cette égalité n'existe pas, puisque l'Etat en tant qu'acteur de la scène international, devient totalement transparent et donc vulnérable. Ensuite, car il ne peut plus garantir la protection des libertés constitutionnelles octroyées à ces citoyens.

Echelon semble alors matérialiser les propos de Marcel Merle : « il faut commencer par détruire un mythe forgé par les juristes (et inscrit aujourd'hui encore dans la Charte des Nations-Unies) : celui de l'« égalité souveraine » des États entre eux. Ce mythe a pour effet de masquer les inégalités de toutes sortes, mais aussi les différences de nature et de rôle qui existent entre les États. Il ne s'agit pas, en effet, de simples contrastes de taille et de puissance, mais aussi de place dans l'échelle des générations, il y a des États " vieux " et d'autres "jeunes", de fonction dans la société et de conception du pouvoir. »[62]

Le constat qui s'impose est que la réciprocité des droits et des avantages, principal implication du principe d'égalité souveraine, n'est pas assurée dans le cyberespace. A l'heure de l'avènement de la société de l'information les conséquences en sont encore plus dommageable pour les Etats victimes de cette inégalité.

On peut même avancer que cette inégalité est présente au sein de l'accord UKUSA, puisque les différents Etats membres n'ont pas un égal accès aux informations qui sont collectées, les Etats Unis assurant le tri et la redistribution de l'information. Cet aspect est notamment mis en lumière par les questions des parlementaires anglais adressées à leur gouvernement : Le 6 avril 1998, Norman Baker: « *Quel mécanisme est en place pour garantir que l'information glanée des interceptions des télécommunications par les forces américaines à Menwith Hill n'est pas utilisée de manière préjudiciable aux intérêts du Royaume-Uni ?* »
Réponse du Ministre des Forces Armées : « *Du personnel anglais est intégré à chaque niveau de Menwith Hill et nous pouvons donc être confiant dans le fait qu'aucune activité préjudiciable aux intérêts du Royaume-Uni ne se déroule là-bas.* »

On pourra répondre au ministre des force armée qu'il ne s'agit pas d'une garantie suffisante, au regard de la perte par Airbus industrie d'un contrat d'une valeur de 6 milliards de dollars au profit de Mac-Donnell Douglas[63]. Le Royaume Uni faisant partie du consortium Air bus, les informations collectées par Echelon et ayant permis à la firme américaine de gagner le marché, ont directement servies à porter atteinte à ses intérêts.

La remise en cause de l'acception traditionnelle de souveraineté est évidente s'agissant du cyberespace, et des flux de données en général, il s'agit maintenant d'apprécier les réponses qui peuvent être apportées.

- **Vers une nouvelle souveraineté à définir**

[62] Un système international sans territoire ?, Marcel Merle, http://www.conflits.org/Numeros/20merle.html
[63] Il s'agissait d'un contrat avec l'Arabie Saoudite portant sur des avions de ligne en 1995, Duncan Campbell, Surveillance Electronique Planétaire, édition ALLIA, p98 / 99

Nous confronterons la compétence territoriale des Etats (qui s'exerce dans le cadre de la souveraineté territoriale, première conception de la notion de souveraineté telle qu'elle est présentée dans l'arrêt Lotus de la Cour Permanente de Justice de La Haye[64]) au fait que les interceptions dans le cadre d' Echelon sont une activité spatialement incoercible.

Rappelons tout d'abord que COMINT et SIGINT ne nécessite pas de violer l'espace territorial des pays visés, car une grande partie des interceptions se fait par captation des messages transitant par satellites[65] et que 40 % du trafic mondial des télécommunications hors Etats-Unis passent par les Etats-Unis et leurs réseaux[66]. Cette dépendance technologique leur facilitant le travail.

Ainsi, les interceptions s'effectuent la plupart du temps sans violer le territoire du pays cible, le recours à la notion de territoire pour garantir la souveraineté de l'Etat et sa compétence exclusive sur ce qui y transite n'est pas pertinent s'agissant des informations qui circulent dans un espace virtuel. Illustration parfaite des propos de Marcel Merle[67], selon lesquelle «le territoire est de plus en plus dévalorisé comme symbole de la souveraineté, comme « attribut » de l'Etat-nation … ».

Emettons l'hypothèse que l'interception soit effectuée sur le territoire national, en France elle tomberait sous le coup de l'article 411-6 du Code pénal, visant les délits de trahison et d'espionnage. La personne physique ou morale se rendant coupable de cet acte se verrait condamnée immédiatement, on pense notamment aux opérateurs et fournisseurs d'accès servant de relais à la NSA. La compétence de l'Etat sur son territoire en matière d'interception existe toujours à condition de la présence physique sur le territoire de son auteur.

Mais comme on l'a vu la grande majorité des interceptions s'effectuent en dehors de l'espace territoriale, dès lors quelle solution se présente à l'Etat pour préserver ses compétences et quelles évolutions du droit international public doivent avoir lieu pour l'y aider ?

On se reportera inévitablement aux travaux de Rolando Quadri, dans le cours qu'il dispensa en 1959 à l'Académie de Droit International de la Haye, sur le Droit International Cosmique, et dont Jean-Jacques Lavenue[68] fait l'analyse suivante : « la notion de souveraineté territoriale, élément essentiel de l'ordonnancement juridique international, ne pouvait plus être retenue dans son acception "spatiale", mais devait être appréhendée en termes "fonctionnels". Observant que certaines activités, par nature, parce qu'incoercibles, ne sont pas susceptibles de relever de l'activité gouvernementale de tous les Etats - à raison d'une classique "souveraineté territoriales" de chacun - mais d'un seul Etat à raison de la nature même de l'activité en cause, il en déduisait la nécessité d'une nouvelle approche du Droit International "à raison des activités" ».

---

[64] Décision du 7 septembre 1927, journal de droit international privé, 1927, p. 1002 et suivantes

[65] L'espace Aérien au-delà de 100 kilomètres appartient au domaine public international et est affecté à l'usage commun de l'ensemble des Etats.

[66] Compte rendu de l'audition de Monsieur Yves Poullet, le 11 octobre 2000 devant le groupe de travail "Société de l'information" du parlement belge, **[PDF]** www.droit.fundp.ac.be/Textes/CCE.pdf

[67] Un système international sans territoire ?, Marcel Merle, http://www.conflits.org/Numeros/20merle.html

[68] Cyberespace et Droit International : pour un nouveau Jus Communicationis, Jean-Jacques Lavenue, http://www2.univ-lille2.fr/droit/enseignements/dess_cyber/index.html

Cette analyse est transposable au cyberespace et aux pratiques COMINT et SIGINT. L'interception des signaux constituent bien un activité spatialement incoercible sur laquelle la souveraineté territoriale n'a pas de prise. D'où la nécessiter de faire évoluer le droit international, afin qu'il délimite le champs des interceptions légalement admissibles.

Cependant tout comme pour la régulation d'Internet cela ne sera possible qu'avec le renforcement de la collaboration internationale, voire qu'avec la coopération des Etats Unis, ce qui est loin d'être acquis. Le droit international seul ne peut rien, il reste suspendu à la volonté des Etats. Il nous faut alors déterminer si l'ensemble de la communauté internationale aura suffisamment de poids pour faire plier les Etats Unis. Tout en gardant à l'esprit que chaque Etat souhaite secrètement bénéficier d'un tel outil ou met déjà tout en œuvre pour l'acquérir.

Dans ce but, nous étudierons l'impact d'Echelon sur les alliances internationales, ce qui nous amènera à traiter de l'ambiguï té des rapport USA / UE, de la volonté hégémonique des Etats Unis.

2 / Quels impacts sur les alliances internationales économiques et militaires ?

Echelon nous fait voir les relations internationales sous un nouvel angle, des alliances sont révélées et des équilibres que l'ont croyaient acquis sont remis en cause. La disparition du bloc soviétique et de ses symboles a emporté avec elle un équilibre international qui s'était construit sur la bipolarité.

Les américains ont alors procédé à une reconversion de leur personnel et de leurs outils vers de nouvelles cibles. On aurait pu croire que les activités COMINT et SIGINT seraient uniquement orienté vers la lutte contre le crime organisé, le terrorisme et la surveillance de quelques pays identifiés comme des ennemis tel que la Libye ou la Corée du Nord.

Mais le rapport de Duncan Campbell révèle une autre réalité, Echelon a été reconverti en grande partie comme un outil d'intelligence économique pour ne pas dire de guerre économique dont la cible première est l'Europe.

C'est pourquoi il nous semble important d'étudier l'impact de la découverte d'Echelon sur les relations internationales, afin de déterminer si les alliances issues de la seconde guerre mondiale supporteront les tentions, et enfin pour entrevoir les objectifs de la logique mise en place par les Etats Unis.

a) Les alliés d'hier sont-ils les ennemis d'aujourd'hui ?

Dans un premier temps nous étudierons les rapports entre les différents membres de l'accord UKUSA, afin de démontrer l'existence d'un véritable pôle Anglo-saxon sous domination américaine. Dans un second temps nous verrons que les alliances militaires ne semblent pas être remise en cause mais qu'elles cohabitent difficilement avec les enjeux économiques.

- **L'affirmation d'un pôle Anglo-saxon sous domination américaine**

Comme nous l'avons vu précédemment Echelon met en présence cinq nations Anglo-saxonnes , deux nations fondatrices qui sont les Etats Unis et le Royaume Uni, et trois autres qui ont intégré le système en cours de route, le Canada, la Nouvelle-Zélande et l'Australie. Ces cinq pays constituent le noyau dur du système. On doit ensuite ajouter l'Allemagne, la Turquie, la Norvège et le Danemark qui après signatures d'accords secrets SIGINT devinrent des participants tiers.

On peut ainsi établir un semblant de hiérarchie au sein de l'accord, les USA se situant en haut de la pyramide, immédiatement suivi par le Royaume Uni, ensuite on peut supposer que le Canada, l'Australie et la Nouvelle-Zélande sont à un niveau quasiment identique. Arrive en queue de peloton les participants tiers qui servent avant tout de relais stratégiques accueillant des installations dans les bases américaines mise en place à la fin de la seconde guerre mondiale.

Cette hiérarchie correspond d'ailleurs aux investissements financiers et humains mis au service du système, ainsi les Etats Unis allouent 4 milliards de dollars et mobilisent 40 000 personnes et la grande Bretagne 500 millions de livres et 15 000 personnes.

L'absence de réciprocité entre les participants peut être illustrée par le système d'échange de « dictionnaires » de mots clés servant à la configuration des ordinateurs, comme l'explique Philippe Rivière dans une série d'articles[69] consacrés à Echelon, parus dans le Monde Diplomatique : « le fait même qu'Echelon permette des échanges de « dictionnaires » aboutit à faire de chaque service de renseignement un agent de collecte, sur son territoire, d'informations destinées à des partenaires étrangers. Mais la transmission se fait de manière automatisée et, en raison du mode de programmation du système, il ne permet pas à la partie néo-zélandaise de connaître les mots-clés utilisés par ses partenaires. La réciproque, on s'en doute, n'est pas vraie... Cela aurait, par exemple, pu permettre aux Etats-Unis d'utiliser les infrastructures néo-zélandaises pour espionner les communications de l'association Greenpeace, lors de sa campagne de protestation contre les essais nucléaires français autour de l'atoll de Mururoa en 1995, sans en informer Wellington ! »

Les Etats Unis ont la main mise sur le système, l'architecture du réseau à été entièrement conçue par la NSA, elle seule possède l'ensemble des codes ou combinaisons d'accès à l'ensemble du réseau. Ainsi, mis à part le Royaume Uni, le Canada, la Nouvelle-Zélande et l'Australie ont des rôles assignés en terme de technologies et de secteurs d'intervention. Toutes les informations sont communiquées à la NSA de manière automatique mais ne sont redistribuées que si elle l'estime nécessaire.

C'est semble-t-il ce déséquilibre dans les relations internes de l'UKUSA qui ont poussé le gouvernement australien à briser le rang en 1999 et à affirmer publiquement que le Defence, Signals Directorate « coopère effectivement avec des organisations équivalentes d'espionnage des signaux outre mer sous l'égide de l'alliance UKUSA »[70]. De même, la Nouvelle-Zélande semble avoir été mis de coté, pour un temps limité, suite à son refus d'accepter des navires nucléaires américains dans ses ports.

---

[69] Le système Echelon, Philipe Rivière, Le Monde Diplomatique, http://www.monde-diplomatique.fr/mav/46/RIVIERE/m1.html

[70] Surveillance Electronique Planétaire, Duncan Campbell, édition ALLIA, p 19

Comme nous l'avons déjà souligné même les Etats membres de l'accord voient leur souveraineté atteinte, participant à un accord multilatérale qui peut leur porter atteinte jusque dans leurs frontières. On peut alors s'interroger sur leurs motivations à rester dans un tel système. La réponse est simple, ils profitent d'une technologie qu'ils ne pourraient acquérir seuls et qui à l'heure de la société de l'information leur procure des avantages décisifs. Les perspectives offertes par des systèmes tel qu'Echelon sont si vastes que chaque Etat souhaite en profiter, quelque soit le prix à payer.

Après avoir vu les relations au sein du pôle constitué autour des Etats Unis, il s'agit d'étudier les relations qu'il entretient avec le reste de la communauté internationale et notamment les pays de l'Union Européenne.

- **L'Europe : allié militaire traditionnel à ménager ou ennemi économique à surveiller ?**

Les conflits d'intérêts entre les Etats Unis et l'Europe, se cristallisent autour des questions économique, la liste est longue, on ne citera que pour exemple la Politique Agricole Commune, ou encore la récente crise de la banane, sans parler de la question des droits d'auteurs ou enfin l'aéronautique. L'Europe constitue le principal rival économique des Etats Unis, mais paradoxalement il s'agit aussi de son premier allié militaire.

Ainsi il serait naï f de croire que les différents gouvernements qui se sont succédés à la tête des plus grandes nations européennes n'aient pas été au courrant d'Echelon ou n'en ait pas profité, d'autant plus que plusieurs Etats sont directement impliqués. Mêmes si certains intérêts diverges chaque Etat semblait préserver le secret afin de pouvoir profiter du système ou développer son propre système plus ou moins autonome des Etats Unis, comme la France par exemple.

D'une part, car la dépendance technologique vis à vis des Etats Unis est immense, et d'autre part car aucune des grandes nations occidentales n'a réellement intérêt à provoquer un débat national et international autour de la question des pratiques COMINT et SIGINT.

Tout d'abord, s'agissant de la perspective d'un débat national, Echelon révèle une fracture entre le pouvoir exécutif et le pouvoir législatifs. Les services de renseignements relevant de la compétence du gouvernement le contrôle par « les représentants du peuple » ne peut s'exercer. La possibilité d'un débat national met mal à l'aise les Etats confrontés aux interrogations et reproches des citoyens et parlementaires, alors qu'il s'agit d'activités secrètes qu'ils entendent garder secrètes.

On citera à titre d'exemple quelques questions réponses des parlementaires anglais : 25 Mars 1994, Mr Cryer *: « Quels droits les individus ou les firmes possèdent-ils s'ils croient être espionnés par Menwith Hill ? Par exemple, le Ministre peut-il nous donner l'assurance formelle que Menwith Hill n'intercepte pas le trafic commercial ? …Finalement, si le Ministre est tellement confiant dans la démocratie, m'autorisera-t-il, moi et d'autres membres du parti travailliste à visiter la base ? »*
Réponse : « *…Comme la Chambre le sait, j'ai visité la station le 27 janvier. J'ai reçu des briefings concernant son rôle actuel de la part du personnel senior américain et anglais travaillant là-bas, celui-ci incluant le chef de la base… Le travail effectué là-bas est très sensible et classifié secret. Je crois très fermement que si je commentais en détail les activités que j'ai vu menées là-bas, cela ne serait pas dans l'intérêt national et nuirait en tout cas à*

l'objectif véritable de ce travail… Il y a actuellement 600 employés britanniques servant à chaque niveau de la base et 1200 employés américains. L'honorable Membre pour Bradford Sud a mentionné des visites de Menwith Hill par des membres du Parlement et des Membres du Parlement Européen. Des demandes antérieures pour de telles visites ou conférences n'ont pas été approuvées sur base des dérangements [que cela causerait] dans le fonctionnement opérationnel de la base et pour des raisons de sécurité. J'ai déclaré qu'il en serait de même tant pour les membres du parti conservateur que pour les membres du parti travailliste. Il n'entre pas dans la pratique du Ministère de la Défense d'organiser des visites guidées des installations de travail de Menwith Hill. Dans ma réponse à la Chambre le 8 mars, j'ai dit que ces restrictions s'appliqueraient à tous [les parlementaires]. »

Le 3 juin 1996, Lord Jenkins of Putney: « *Des interceptions de télécommunications sont-elles effectuées par la NSA américaine à Menwith Hill ? Et, dans l'affirmative, quels messages sont interceptés et pour quelle finalité ? »*
Réponse *: « Il n'entre pas dans la politique du gouvernement de commenter les opérations détaillées menées à Menwith Hill. En tous cas, aucune activité considérée comme hostile aux intérêts britanniques n'est, -ou ne serait-, permise dans cette station. »*

Cette étanchéité qui semble exister dans le domaine des renseignements témoigne de l'hypocrisie générale dans laquelle s'est déroulée la découverte d'Echelon, seul le grand public voire quelques parlementaire sont tombés des nues. C'est pourquoi on peut affirmer que les alliances militaires ne semblent pas devoir être remise en cause, notamment si l'on s'attarde sur le projet de politique étrangère et de sécurité commune incluant l'ensemble des questions relatives à la sécurité de l'Union. En effet, l'article 17 du traité de Nice prévoit explicitement de respecter les engagements pris dans le cadre de l'OTAN[71] et donc confirme les liens avec les Etats Unis.

[71] «Article 17 : 1. La politique étrangère et de sécurité commune inclut l'ensemble des questions relatives à la sécurité de l'Union, y compris la définition progressive d'une politique de défense commune, qui pourrait conduire à une défense commune, si le Conseil européen en décide ainsi. Il recommande, dans ce cas, aux États membres d'adopter une décision dans ce sens conformément à leurs exigences constitutionnelles respectives. La politique de l'Union au sens du présent article n'affecte pas le caractère spécifique de la politique de sécurité et de défense de certains États membres, elle respecte les obligations découlant du traité de l'Atlantique Nord pour certains États membres qui considèrent que leur défense commune est réalisée dans le cadre de l'Organisation du traité de l'Atlantique Nord (OTAN) et elle est compatible avec la politique commune de sécurité et de défense arrêtée dans ce cadre. La définition progressive d'une politique de défense commune est étayée, dans la mesure où les États membres le jugent approprié, par une coopération entre eux en matière d'armements.
2. Les questions visées au présent article incluent les missions humanitaires et d'évacuation, les missions de maintien de la paix et les missions de forces de combat pour la gestion des crises, y compris les missions de rétablissement de la paix.
3. Les décisions ayant des implications dans le domaine de la défense dont il est question au présent article sont prises sans préjudice des politiques et des obligations visées au paragraphe 1, deuxième alinéa.
4. Le présent article ne fait pas obstacle au développement d'une coopération plus étroite entre deux ou plusieurs États membres au niveau bilatéral, dans le cadre de l'Union de l'Europe occidentale (UEO) et de l'OTAN, dans la mesure où cette coopération ne contrevient pas à celle qui est prévue au présent titre ni ne l'entrave.

Nonobstant, la nécessité de clarifier les cibles et les objectifs de COMINT et SIGINT est plus que jamais primordiale si l'on veut empêcher les Etats Unis de nous reléguer au rang de faire valoir, et surtout si l'on veut préserver les libertés des citoyens du monde et le développement de l'Union Européenne.

b) Echelon : Les moyens d'une tyrannie totale à la portée des USA

La dépendance croissante de la société à l'égard de l'information électronique donne aux USA « le pouvoir d'instaurer une tyrannie totale » comme le soulignait déjà un sénateur américain en 1975 suite à l'enquête du Sénat américain sur la NSA.

En effet, comme nous l'avons vu les Etats Unis ont la maîtrise technologique civile et militaire, ce qui leur assure un contrôle des infrastructures, leur compétence est planétaire et ne semble pas en pratique pouvoir être remise en cause. D'autant plus si l'on prend en considération la manière dont les membres de la commission temporaire européenne ont été reçus. Cette dernière a quitté Washington précipitamment jeudi 10 mai, suite à l'annulation à la dernière minute des rendez-vous prévus avec le Département d´Etat américain[72], le Département du commerce et les services de renseignements américains.

On peut comprendre la réaction de Carlos Coelho qui dirige cette commission : "*Nous sommes très déçus par le refus de dernière minute de la CIA (Central Intelligence Agency) et la NSA (National Security Agency) de rencontrer notre délégation en dépit préparatifs avancés qui avaient été effectués. En conséquence, nous écourtons notre visite à Washington et retournons en Europe immédiatement* "[73].C'est à la même fin de recevoir que c'était vu confronté la commission de la Défense nationale et des Forces Armées présidée par Paul Quilés. Ce qui tend à démontrer que les Etats Unis souhaitent garder jalousement leurs prérogatives sans avoir à rendre de comptes.

Enfin, s'il fallait encore une preuve que les Etats-Unis souhaitent imposer une véritable *« lex Americana »* aux flux informationnels on se référera au projet NIMA[74]. Dont Paul Virilio[75] fait une étude assez détaillée : « A la fin de l'année 1996, à côté de la National Security Agency (NSA) (…) les Etats-Unis lançaient une agence nouvelle : la National Imagery and Mapping Agency (NIMA). Regroupant près de 10 000 personnes, cette agence, dépendant du Pentagone, devait centraliser l'ensemble des vues captées par les satellites militaires et oeuvrer à l'élaboration d'un standard de traitement numérique de ces images, nommé NIFTS. Permettant la transmission d'images en temps réel, ce standard devait initialement ne concerner que les utilisateurs relevant du département de la défense et du renseignement, mais l'importance de l'observation spatiale et sa rationalité économique ne devaient pas échapper longtemps aux théoriciens de la cyber-guerre *(infowar)*. Dès 1997, la NIMA décidait donc de participer au programme « Global Information Dominance », dont l'objectif est de contrôler l'exploitation du flux de l'imagerie commerciale dans le monde. Dans ce but, l'Agence accorde

---

5. En vue de promouvoir la réalisation des objectifs définis au présent article, les dispositions de celui-ci seront réexaminées conformément à l'article 48.»

[72] L´équivalent de notre ministère des affaires étrangères

[73] Echelon : la NSA pose un lapin à l´Europe, Eric Mugneret, transfert.net, http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=5579

[74] National Imagery and Mapping Agency (NIMA)

[75] Télésurveillance globale, Paul Virilio, le Monde Diplomatique Août 1999, http://www.monde-diplomatique.fr/1999/08/VIRILIO/12332.html

jusqu'à 5 millions de dollars aux entreprises, tant américaines qu'étrangères, rendant inter-opérables leurs systèmes de traitement de données et s'engageant à respecter des délais très courts de fourniture des images. La NIMA rediffuse ensuite ces documents vers les militaires des Etats-Unis, mais aussi vers des clients civils, américains ou étrangers. Devenir ainsi le point de passage obligé des images commerciales, par le biais d'une politique d'achat et de distribution à grande échelle, c'est donc la parade trouvée par le Pentagone et la Central Intelligence Agency (CIA) pour entraver la mise en place d'un marché libre de l'imagerie spatiale. »
Il s'agit de la dernière touche à un grand projet d'ensemble n'ayant pour objectif que d'assurer aux « maîtres du monde » le contrôle technique et économique de l'ensemble des télécommunications internationales, grâce à cette agence de télésurveillance globale la panoplie américaine semble complète.

Cependant, au regard des enjeux économique et surtout au regard de la protection des libertés individuelles et publiques il est fondamental que la communauté internationale politique et civile se mobilise afin d'engager un débat initiateur de réforme de fonds, dont la pierre angulaire devrait être la définition d'un ordre public international.

B / Les atteintes aux droits des personnes privées

1/ une remise en cause des libertés fondamentales des individus

a) <u>Le difficile respect des législations</u>

Les législations protectrices de la vie privée des individus sont nombreuses. Le droit au respect de la vie privée figure dans le texte qui est sensé servir le référence à tous les Etats en matière de droits fondamentaux : la déclaration universelle des droits de l'homme. En son article 12, elle énonce en effet que *« nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance (…). Toute personne a le droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». De même, le Pacte International du 19 décembre 1966 relatif aux droits civils et politiques prescrit en son article 17 que: *« Personne ne sera soumis à des interférences arbitraires et illégitimes qui iraient à l'encontre de sa vie privée (…). Chacun a le droit à une protection légale contre de telles interférence*s ». Bien qu'ainsi affirmé, le principe n'est pourtant pas respecté de la même manière dans les différents continents.

a Une grande variété de dispositifs législatifs….

♦ Les dispositions de la Convention européenne des droits de l'homme

L'interception de messages transmis par télécommunications représente un danger tant pour la vie privée des personnes mises sur écoutes que pour leur liberté d'expression. Ces deux libertés représentent des libertés essentielles dont la protection est assurée par nombre de textes internationaux dont la Convention européenne des Droits de l'Homme. Certes, comme on l'a vu précédemment, des impératifs légitimes de sécurité de l'Etat justifient que les Etats disposent de moyens techniques efficaces permettant l'interception légale des télécommunications.

Cependant comme le note l'arrêt Klass[76], il est nécessaire de disposer *« de garanties suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendr*e ». Quatre conditions dès lors limitent l'immixtion possible de l'Etat. Ces quatre conditions applicables en matière d'interception des télécommunications ont été maintes fois rappelées par la jurisprudence de la Cour européenne des droits de l'Homme. Ainsi, il importe:

1° que l'interception n'ait lieu que dans le cadre des objectifs d'intérêt vital de l'Etat énumérés par la Convention elle-même tant dans l'article 8 que dans l'article 10;

[76] CEDH, Klass v. Germany 6 septembre 1978

2° que ces finalités soient prévues par la loi, c'est-à-dire par un texte réglementaire accessible au public et rédigé de façon suffisamment précise pour que le citoyen puisse y répondre par un comportement adéquat (arrêt Kruslin 24 avril 1990);

3° que la mesure prise soit strictement proportionnée à l'objectif poursuivi. A cet égard, comme le répètent notamment les arrêts Klass et Leander[77], une surveillance exploratoire ou générale effectuée sur une grande échelle est prohibée;

4° enfin selon l'arrêt Leander rendu à propos de la contestation d'un citoyen convaincu d'être fiché par la sûreté de l'Etat et se voyant opposer lors de sa demande d'accès à son dossier, le dogme du secret indispensable à la sécurité de l'Etat, il importe qu'une balance soit opérée entre d'une part la protection de la vie privée et d'autre part les impératifs de sécurité et d'ordre public qui fondent la mission des services de renseignements et de sûreté; importe plus encore, ajoute l'arrêt, que cette balance soit opérée par une autorité indépendante.

A propos des interceptions de télécommunications, précisément, la recommandation R(95)14 du Comité des Ministres du Conseil de l'Europe adoptée le 11 septembre 1995 « relative à la procédure pénale en rapport aux technologies de l'information » préconise entre autres que les lois pénales soient modifiées pour permettre l'interception en cas d'investigation lors d'attaques sérieuses contre les systèmes d'information et de télécommunications et que des mesures soient prises pour minimiser l'impact négatif de la cryptographie sans remettre en cause son utilisation au-delà de ce qui est nécessaire. pour qu'il y ait conformité aux exigences des principes du Conseil de l'Europe, il faut :

- que la (ou les) finalité(s) d'Echelon soi(en)t définie(s) par des textes réglementaires, clairs et accessibles au public.
- que les interceptions réalisées dans le cadre d'Echelon n'aient pas lieu sur base de la recherche systématique de mots clés ou selon d'autres critères généraux, mais, comme le prescrit la jurisprudence de la Cour européenne des droits de l'Homme, en fonction de critères spécifiques liés à des infractions précises ou à leurs auteurs supposés.
- qu'un tel système limite strictement la collecte de données à ce qui est nécessaire aux finalités de sûreté de l'Etat.
- qu'il soit analysé si un contrôle des écoutes par une autorité indépendante est prévu (24) conformément à l'exigence de l'arrêt Léander de la Cour européenne des Droits de l'Homme.

♦ La position de l'Union Européenne au regard de la vie privée

L'article 6 du Traité sur l'Union européenne affirme que *« L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la CEDH, signée à Rome le 4 novembre 1950(…) »*. Le traité d'Amsterdam complète cette disposition en son article 46, qui donne une compétence juridictionnelle à la CJCE pour vérifier le respect des droits fondamentaux garantis à travers la référence que l'article 6 fait à la CEDH.

[77] CEDH, Leander 25 février 1987

Néanmoins cette reconnaissance des droits fondamentaux de la CEDH est récente. En effet, le Conseil de la Communauté européenne avait adopté, sous la pression américaine, le 17 janvier 1995, une résolution visant à faciliter les écoutes téléphoniques[78]. Celle-ci détaille les conditions techniques nécessaires à l'interception des télécommunications, sans aborder la question des conditions dans lesquelles de telles interceptions devraient avoir lieu. Cette résolution prise à la hâte et sans contrôle parlementaire a été remise en question récemment par le Parlement, qui tire en la matière les conséquences de l'adoption du traité d'Amsterdam.

A contrario, la Résolution du Parlement européen du 16 septembre 1998 vise précisément les relations transatlantiques et le système Echelon en particulier et conclut que, nonobstant l'importance de telles relations et des objectifs supposés du système Echelon, *« il est essentiel que l'on puisse s'appuyer sur des systèmes de contrôle démocratique en ce qui concerne le recours à ces technologies et les informations obtenue*s ».

Le 3 mai 1999, le groupe de Protection des personnes à l'égard du traitement des données personnelles émettait une recommandation concernant le respect de la vie privée dans le contexte de l'interception des télécommunications. Cette recommandation rappelle le principe du secret des communications et note que celui-ci est garanti par la directive 97/66/CE qui crée pour les Etats membres une obligation de garantir le secret des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessibles au public. Dans son article 14 paragraphe 1, la directive 97/66/CE précise que les Etats membres ne peuvent limiter l'obligation de confidentialité des communications sur des réseaux publics que lorsqu'une telle mesure constitue une mesure nécessaire pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales. Ainsi, si exception il y a, celle-ci est de stricte interprétation et suppose que l'écoute soit le moyen indispensable à l'objectif recherché.

Les dispositifs en Europe prévoient donc le respect de la vie privée et l'encadrement des interceptions de télécommunications dans un cadre strict et des cas limités. Mais les interceptions effectuées dans le cadre du système Echelon dépendent en particulier des Etats-Unis, dont la conception en matière de vie privée est beaucoup plus laxiste.

- La conception américaine en matière de vie privée

Les Etats-Unis sont souvent considérés comme l'Etat du libéralisme. En matière de vie privée aussi, cette réputation se vérifie. Il n'est en effet pas rare de voir la liberté d'expression mise en avant, au détriment du respect de la vie privée. On ne peut contester la propension des Américains à voir la vie des uns et des autres étalées dans la presse.

[78] Résolution du Conseil 17/1/95, J.O. C. 329 du 4 novembre 1996 p. 1 à 6, votée sans l'avis du Parlement

Les Etats-Unis sont également le pays de la régulation par l'économie, par le marché. Il n'est donc jamais vu d'un très bon œil un excès de législation, d'autant plus celle-ci a pour but de créer des contraintes et de mettre des entraves au commerce. En effet, ce sont les dispositions en matière de vie privée qui, en Europe, limitent la constitution de fichiers nominatifs. Aux Etats-Unis, ces dispositions ne sont vues que comme un moyen de limiter la publicité et donc comme une entrave au marché.

La tradition américaine est effectivement tournée vers l'autorégulation. S'il n'existe pas, comme l'a rappelé Mme Carblanc lors de son intervention à propos de la politique de l'OCDE en matière de données personnelles[79], de loi générale visant à protéger la vie privée, la Federal Trade Commission n'en est pas moins un outil important qui tente de faire respecter les principes de protection des données personnelles, mais cela en ce qui concerne les agissements des entreprises commerciales, et non ceux des autorités.

Les écoutes tous azimuts restent typiquement un réflexe américain. Selon une enquête de l'American Management Association, en 1999, 73.5 % des entreprises installées aux Etats-Unis surveillaient les communications de leurs salariés. Mais cette conception semble en voie de transformation. Un sondage[80] réalisé au début de cette année montre que 62 % des Américains pensent que de nouvelles lois devraient être adoptées afin d'assurer que les citoyens « ordinaires » voient leur vie privée protégée vis-à-vis des agences gouvernementales.

Si la conception de la protection de la vie privée n'est pas la même entre l'Europe et les Etats-Unis, il n'en demeure pas néanmoins que chacun abrite des démocraties et que des droits y sont accordés aux citoyens. En matière d'écoutes téléphoniques, des dispositions sont prises pour éviter les écoutes arbitraires. Ces dispositions varient d'un pays à l'autre, comme on peut le voir à travers l'examen de législations en vigueur en France et aux Etats Unis.

b …qui n'empêchent pas toute atteinte aux droits des individus.

♦ La violation des textes existants

Si des cadres contraignants existent pour protéger les individus des immixtions arbitraires dans leur vie privée, malheureusement ces derniers ne sont pas toujours respectés. En effet, les nombreuses révélations faites par les anciens personnels des agences américaines, qu'ils soient liés à Echelon ou à carnivore, ont montré l'existence de dérives qui ont de quoi effrayer les défenseurs des libertés.

[79] Intervention du 14 mai 2000, dans le cadre du séminaire sur la protection des données personnelles du DESS droit et cyberespace de l'université de Lille II

[80] Sondage "Fear of Online Crime: Americans support FBI interception of criminal suspects' email and new laws to protect online privacy" réalisé par le Pew Internet & American Life Project, 1er février – 1er mars 2001

Comme on l'a vu, pour le FBI, qui a la main sur le Carnivore, seuls les contenus des messages des personnes incriminées sont enregistrés et peuvent être lus par des yeux humains, le reste étant seulement trié puis écarté par l'ordinateur.

Cependant, selon l'ACLU, « le FBI peut lire l'ensemble du trafic passant par les ordinateurs du serveur, c'est comme si toutes les communications téléphoniques d'un opérateur étaient écoutées ». En outre, Wayne Madsen, ancien membre de la NSA, reconnaît qu'il est facile de contourner les obligations légales : « les enquêteurs peuvent tirer parti de mandats d'écoutes, aussi faciles à obtenir qu'un tampon. Par exemple, pour une écoute téléphonique, cette procédure limite l'interception au numéro appelé et au numéro appelant. Nous savons que le FBI a utilisé ce type de mandat pour capturer des e-mails. Officiellement, le FBI affirme qu'il ne capture que l'adresse de l'expéditeur et du destinataire. Mais l nous prend pour des naï fs : avec des systèmes de type webmail de Hotmail, par exemple, on peut aussi récupérer le sujet du message et même son contenu »[81]

Les interceptions menées par Echelon sont en effet pilotées à partir de mots-clés, et non pas en plaçant sous surveillance systématique des numéros de téléphone, de fax, ou des adresses Internet de personnes précises. Cet aspect technique, certes très prometteur en termes de renseignement, efface toute possibilité de définition - par décision judiciaire, militaire ou politique - de la source surveillée : toute personne est susceptible d'être écoutée pour peu que sa conversation soit jugée « intéressante » par le logiciel ! Les dérives sont inévitables. Un ancien espion canadien, M. Mike Frost, accuse ainsi Mme Margaret Thatcher d'avoir fait venir à Londres, en février 1983, des opérateurs canadiens pour surveiller deux des ministres de son propre gouvernement qui, naï fs, préparaient quelque trahison politique en communiquant avec leurs téléphones mobiles.

De même, le Free Congress Research and Education Fondation rapporte qu'Echelon n'est pas demeuré inactif au Canada par exemple : A Ottawa, il s'est agi de découvrir si Margaret Trudeau, la femme du premier ministre, consommait de la marijuana.

En outre, les filtres employés par la Police pour rester dans le cadre de leur mandat et laisser de coté les messages non-désiré peuvent être changés à distance sans que le fournisseur d'accès en soit informé. Les services de renseignement ont donc une importante marge de manœuvre.

Il est évidemment tentant d'utiliser un système si secret et si puissant pour les renseignements généraux et les opérations de basse police : en 1992, des opérateurs de haut rang des services secrets britanniques, fâchés de certaines dérives, dévoilèrent qu'Amnesty International, entre autres organisations non gouvernementales, avait été écoutée à partir de mots-clés relatifs au trafic d'armes

[81] Entretien pour Libération, 7 et 8 octobre 200, par Edouard Launet

Non seulement les personnes physiques, mais aussi les personnes morales peuvent donc voir leurs libertés remises en cause par le système Carnivore. On peut penser en effet aux FAI qui sont dans l'obligation d'installer sur leur serveurs le dispositif Carnivore lorsque le FBI le leur demande.

Ainsi, le serveur EarthLink, le deuxième plus important aux Etats-Unis, avait refusé de laisser le Fbi installer son système, mettant en avant des questions de libertés publiques. Mais un juge l'a sommé d'accepter les écoutes du FBI. Les entreprises ne sont donc plus libres de protéger les données de leurs clients, ce qui peut leur porter préjudice en terme d'image.

- ♦ l'exploitation du vide juridique au plan international

Si le IVème amendement à la Constitution des Etats-Unis garanti le respect de la vie privée pour les citoyens américains, il ne le garanti pas pour les citoyens des autres Etats. Pour cette raison, la NSA américaine ne doit demander aucune autorisation lorsqu'elle veut intercepter les communications qui traversent la planète.
En effet la vie privée des individus est peu protégée au niveau international. Si la déclaration universelle des droits de l'homme de 1948, ainsi que le pacte des droits civils et politiques de 1966, affirment le droit au respect de la vie privée, ces textes sont insuffisamment contraignants.

Comme on l'a vu, les conceptions étatiques en matière de vie privée varient d'un Etat à l'autre. Une illustration de ces variation et du vide juridique réside dans l'instauration du Safe Harbor.

L'accord Safe Harbor a été scellé le 15 mars 2000 entre la Commission européenne et le Département au Commerce américain. Il trouve son origine dans la directive 95/46/CE en matière de flux transfrontaliers : celle-ci fait obligation aux états membres de veiller à ce que les données personnelles soient transmises vers des Etats dont le niveau de protection est suffisant. La commission apprécie si le pays offre la protection adéquate.

En l'absence de dispositif contraignant et uniforme au niveau international, un accord bilatéral a donc été passé en mars 2000, prévoyant que les entreprises qui respectent certaines conditions définies en matière de protection des données personnelles peuvent entrer dans la sphère du Safe harbor, et que des transfert de données personnelles pourraient donc être effectués vers elle à partir d'entreprises européennes.

Cependant, en mars 2001, le Congrès américain a remis en cause cet accord, au motif que les dispositions prévues par la Commission Européenne étaient beaucoup trop contraignantes.

Cet exemple illustre donc parfaitement les difficultés qu'ont les Etats a uniformiser leurs politiques en matière de protection de la vie privée, et cela dans un contexte dans lequel aucune disposition générale n'est prévue au niveau international.

b) Les tentatives de lutte contre les atteintes

a Les sanctions judiciaires

Si l'on considère que le mode opératoire des systèmes de surveillance constitue des violations caractérisées et permanente de la vie privée, alors tout citoyen concerné et victime de tels agissements est fondé à porter plainte.

On peut ainsi imaginer, en France, de porter plainte auprès du Procureur de la République de son domicile. En effet les articles 226-2 et 226-15 du code pénal punissent d'1 an d'emprisonnement et de 300 000 F d'amende le fait de «conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document émis obtenu à l'aide de l'un des actes prévus par l'article 226-1 » ainsi que « le fait commis de mauvaise foi, d'ouvrir, de supprimer de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, et d'en prendre frauduleusement connaissance ».

En outre, l'article 432-9 du même code aggrave ces peines lorsqu'elles ont été commises, hors les cas prévus par la loi, par « une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ».

Un citoyen qui aurait fait l'objet d'écoutes par le système Echelon pourrait donc invoquer ces articles afin de voir les responsables des écoutes condamnés.

Le principe semble évident, mais lé réalité est toute autre. Comment espérer voir reconnaître les droits du citoyen injustement « écouté ». D'abord, il faut être conscient du fait d'avoir été écouté, ce qui n'est pas évident quand on sait que le système Echelon existe depuis le début des années 1970 et qu'il n'a été révélé qu'en 1998 au grand public. Ensuite, il faut pouvoir identifier un responsable et le traduire devant les juridictions françaises, ce qui reviendrait en fait à faire condamner la NSA américaine ou l'un des services de renseignement du pacte UKUSA, ce qui n'est en réalité que peu envisageable.

Néanmoins, un collectif d'internautes, baptisé Akawa, soutenu par deux avocats spécialistes de la question, Jean-Pierre Millet et David Nataf, ont porté plainte contre X afin de faire la lumière sur « les violations du secret des correspondances [82]» occasionnées par Echelon. Le Procureur de Paris, Jean Pierre Dintillac, le 24 mai 2000, a mandaté la DST pour enquêter sur l'espionnage généralisé de nos correspondances par les anglo-saxons.

Si elle est possible, on s'aperçoit néanmoins que la lutte contre les atteintes à la vie privée prendra difficilement place dans le contexte judiciaire. C'est donc la société civile qui va tenter de limiter les excès des systèmes de surveillance.

[82] Cité dans Transfer.net, « La France et l'Europe se penchent sur Echelon », par Jean-Marc Domenach, 5 juillet 2000

b Les pressions exercées par la société civile

Dès la révélation (plus ou moins) officielle de l'existence des systèmes Echelon et Carnivore, des levées de boucliers se sont mises en place. Sur la Toile en particulier, des collectifs ont pris naissance pour dénoncer la surveillance globale et alerter la population internaute. C'est par exemple le cas du site « Contre Echelon[83] » qui propose de signer une pétition électronique et qui encourage tous les internautes à inscrire des mots clés dans leurs mails, tels que « bombe », « attentat » ou « Saddam Hussein ». En 1999, certains activistes ont même proposé un «Jam Echelon Day ». Son objectif était d'engorger le Réseau en incitant les internautes à truffer leurs courriers électroniques de ces mots clés susceptibles d'intéresser les services américains.

Des trophées ont été également décernés aux organismes jugés comme mettant le plus en péril les libertés individuelles : Ce sont les BIG BROTHER AWARDS, qui ont récemment élu le système de surveillance Echelon comme l'un de ces organismes.

Parmi les groupes d'action opposés à Echelon, on trouve en particulier les associations de défense des droits civils. Aux Etats-Unis, l'EPIC (Electronic Privacy Information Center) et l'ACLU (American Civil Liberty Union), deux importantes organisations non-gouvernementales, se penchent depuis plusieurs mois sur le dossier.

Après le « déclassement » de documents secrets du FBI en 1998, l'EPIC, alertée par les possibilités du système Carnivore, avait obtenu d'un juge fédéral, en vertu de la Loi sur L'Accès à l'Information (Freedom of information Act, 1967), que le FBI divulgue toute l'information dont elle dispose sur le système. Un premier rapport a donc été rendu public, mais le FBI a toujours refusé de dévoilé le code source, seul élément qui permettrait de connaître exactement les pouvoirs de Carnivore.

Devant la pression des associations, et donc de l'opinion publique, le Ministère de la Justice s'est saisi de l'affaire. L'Attorney General Janet Reno a demandé une expertise indépendante sur Carnivore. Des experts de l'ITT Research Institute ont donc été mandatés et, dans un récent rapport, ont estimé qu'il n'enfreignait pas le respect de la vie privée et des libertés individuelles. « Il n'apporte aux enquêteurs rien de plus que ce qu'autorise la permission délivrée par la justice » conclut leur rapport.

Cependant, la partialité de ce rapport a rapidement été mise en cause. En effet il s'est avéré que les experts avaient auparavant tous été sous contrat avec le gouvernement, le département de la défense ou encore la NSA[84].

[83] http://www.chez.com/nonguerre/info.htm

[84] Cette information a été révélée à la suite d'une erreur des rédacteurs du rapport : une barre noire masquait le nom et les qualités des experts. Or, un simple copier-coller de Acrobat Reader vers Word laissait apparaître ces données que le FBI voulait dissimuler !

Le Congrès s'est alors à son tour saisi du dossier. C'est en effet le Congrès qui alloue des fonds aux systèmes de surveillance. Selon les dires de Dick Arney, président du groupe Républicain à la Chambre des Représentants, «les experts ont blanchit les méfaits du système Carnivore ». Le Congrès américain a donc commencé une série d'audition à l'automne 2000 afin de déterminer quels étaient les risques encourus au niveau des libertés fondamentales et le gouvernement a promis de lui présenter plusieurs projets de loi visant à protéger les correspondances et en particulier les e-mails. Mais le changement de gouvernement en ce début d'année risque bien d'avoir quelque peu perturbé ces résolutions.

2 / les atteintes aux droits des entreprises

a) de l'espionnage militaire à l'espionnage économique…

Comme on l'a déjà évoqué, d'un but militaire, le système Echelon a ensuite était affecté à un but plus économique : l'espionnage commercial. Celui-ci est en effet devenu une priorité sans cesse accrue à partir des années 1960. En effet, en 1970, Gérard Burcke, au nom du Conseil Consultatif des renseignements Extérieurs, recommandait : « dorénavant l'espionnage commercial devra être considéré comme une fonction de la sécurité nationale, jouissant d'une priorité équivalente à l'espionnage diplomatique, militaire et technologique »[85].

En 1977 fut d'ailleurs crée un Bureau de liaison des renseignements[86] au sein du Département américain du commerce.

Puis c'est surtout avec le début des années 1990 que l'Etat américain a commencé à se soucier des intérêts privés de ses entreprises, dans le but de restaurer leur compétitivité, et cela en opposition avec la tradition libérale américaine. Sous la présidence de Georges Bush est donc préconisé d'effectuer une surveillance des activités des firmes et gouvernements étrangers dans les secteurs clés de l'économie, afin de mettre en place un système d'alerte avancé. Les organes de renseignement sont conviés à contribuer de manière significative à ce type d'efforts[87].

Cette politique de veille concurrentielle se traduit par la mise en oeuvre du cycle du renseignement, appliqué cette fois aux entreprises étrangères. En premier lieu, un état des lieux des secteurs clés de l'industrie américaine et de leurs besoins en renseignements est effectué.

Puis la phase de recherche des informations est mise en oeuvre, c'est là que les autorités ont recours au système d'écoutes généralisé.

[85] Citation extraite de l'émission « Dispatches : the Hill », Channel 4 télévision (GB), 6 octobre 1993.
[86] Office of Intelligence Bureau, crée le 5 mai 1977 entre la NSA, la CIA et le Département du commerce.
[87] Programme cité dans François David, Les échanges commerciaux dans la nouvelle économie mondiale, PUF, 1994

Ensuite l'information est traitée, analysée par des techniciens compétents en la matière, dans le cas d'Echelon par l'un des 38 000 employés de la NSA.

Enfin les informations sont diffusées en fonction des besoins, c'est à dire que des informations recueillies sur une entreprise déterminée seront transmises à sa concurrente directe aux Etats-Unis[88].

Ce retournement vers une politique agressive s'est vu institutionnalisé par le Trade Act de 1988, qui conduit à une redéfinition unilatérale des règles du jeu en matière commerciale. Les dispositions de la section 301 en particulier rendent les règles antidumping et anti-subventions plus contraignantes pour les partenaires commerciaux des Etats-Unis. Cette adoption de ce qui fut alors appelé « le super 301 » fut d'ailleurs a l'origine du blocage de nombreuses négociations avec l'Union Européenne.

Alors même qu'il prenait des dispositions pour empêcher les autres Etats de subventionner leurs entreprises, le gouvernement américain collaborait avec les siennes afin de leur fournir les renseignements nécessaires pour concurrencer les entreprises européennes.

La question de savoir si les services de renseignement américains devaient systématiquement servir les intérêts économiques du pays a été tranchée avec l'élection de Clinton en 1993. celui-ci a alors lancé une politique de « soutien agressif aux acheteurs américains dans les compétitions mondiales là où leur victoire est dans l'intérêt national »[89]. La nouvelle politique, nommée symboliquement « aplanissement de terrain », impliquait des arrangements pour le collectage, la réception et l'utilisation de renseignements secrets au bénéfice du commerce américain. L'Office of Intelligence Support fut transformé en Office of Executive Support, au sein duquel figuraient des membres de la CIA. Ce bureau fournissait des résumés officiels des informations recueillies et les transmettait aux entreprises. Selon Loch K. Johnson, « au commerce, aucun code, aucun livre ne stipule quelles informations peuvent être transmises à une compagnie américaine, ni à quel moment »[90].

Le rapport du journaliste Duncan Campbell au parlement Européen est riche en exemple de marchés détournés de l'Europe au profit des entreprises américaines, et cela grâce à des renseignements obtenus par le système Echelon. Sans les citer tous (Voir le tableau ci-dessus), on peut en reprendre quelques faits marquants.

M. Woolsey, ancien directeur de la CIA cite ainsi, dans un entretien accordé au Wall Street Journal[91], l'affaire SIVAM. La firme française Thomson-CSF avait perdu, à la dernière minute et suite à des accusations de corruption mise en évidence par Echelon, le marché de la surveillance aérienne de l'Amazonie. Le contrat de 1,4 milliards de dollars, aux juteuses

[88] Cycle du renseignement extrait de Philippe Oberson, l'Internet et l'intelligence économique, Les Editions d'Organisation, 1997.
[89] Cité par Duncan Campbell, surveillance économique planétaire, Allia 2001, p. 91
[90] Cité par Scott Shane, «Mixing business with spying ; secret information is passed routinely to U.S. », Baltimore Sun, 1er novembre 1996

commissions, s'envola au profit de Raytheon, un important contractant du département de la défense américain, et l'un des principaux fabricants du système Echelon.

La firme est en effet en charge de la maintenance et des services d'ingénierie de la station d'interception satellite de Sugar Grove, et emploie des spécialistes SIGINT à la base terrestre d'interception des satellites de Denver. (Justifiant l'affaire par la corruption existante en Europe, M. Woolsey oublie toutefois de rappeler que, en novembre 1995, quelque temps après cet épisode, la presse brésilienne publiait des transcriptions d'écoutes téléphoniques, probablement réalisées par la NSA, mettant en cause les tentatives de corruption d'un officiel brésilien par Raytheon)

On peut d'ailleurs noter que, dans un rapport remis, début novembre 1998, au Congrès, le chercheur Patrick S. Poole[92] montre que les principales firmes bénéficiant du produit de l'espionnage mené par Echelon sont celles qui fabriquent l'équipement du réseau Echelon, notamment Lockheed, Boeing, Loral, TRW et Raytheon.

Le résultat le plus saisissant de la politique Clinton d'aplanissement de terrain se produisit en 1994 lorsque notre 1er ministre de l'époque, M. Edouard Balladur, s'envola pour Ryad afin de conclure une vente d'arme et d'avions pour un montant de 6 milliards de dollars. La NSA s'est alors emparée de tous les fax et appels entre le consortium Airbus et le gouvernement Saoudien. La NSA découvrit que les agents d'Airbus offraient des pots-de-vin à un officiel Saoudien. Les autorités américaines, alors mises au courant, appuyèrent la proposition de Boeing et Mc Donnel-Douglas, qui triomphèrent donc[93].

[91] Texte publié par The Wall Street Journal Europe, Bruxelles, 22 mars 2000

[92] Patrick S. Poole, « Echelon : America's Secret Global Surveillance Network », The Privacy Papers, n° 4, novembre 1998, Free Congress Research and Education Foundation, Washington, DC

[93] Information révélée par Scott Shane et Tom Bowman, « America's fortress of spies », Baltimore Sun, 3 décembre 1995

CONTRATS REMPORTES GRACE A LA POLITIQUE AMERICAINE DE « SOUTIEN »

ANNEE	SECTEUR INDUSTRIEL	PAYS ACHETEUR	VALEUR (millions$)	COMPAGNIE AMERICAINE VICTORIEUSE	GROUPE EUROPEEN VAINCU
1994	Protection environnement (SIVAM)	Brésil	1 400	Raythéon	Thomson CSF
1994	Satellites de télécoms.	Arabie saoudite	4 000	AT&T	France
1994	Câbles de fibres optiques	International	1 400	Nynex	France et Singapour
1994	Electricité	Indonésie	2 600	Mission Energy	Non spécifié
1995	Electricité	Tunisie	120	General Electric	“firmes françaises”
1995	Avions de ligne	Arabie Saoudite	6 000	Boeing et Mc Donnell Douglas	Airbus industries
1995	Télécommunications	Emirats arabes Unis	119	AT&T	Alcatel
1996	Incinération d’ordures	Taiwan	226	Westinghouse Electric	“un oligopole européen”
1996	Environnement	Liban	0.3	Ecodit	Anglais, Français, Néerlandais, Danois
1996	Electricité	Israël	300	Mid Atlantic Energy	“compagnies européennes”
1997	Système de contrôle du trafic aérien	Pérou	12	Northrop Grumann	Thomson CSF

Tableau tiré de Duncan Campbell, Surveillance électronique planétaire, Allia, 2001

b) …en violation des principes internationaux de régulation du commerce

♦ La violation des principes du GATT

Bien qu'ils veuillent s'en cacher, les services secrets Américains mettent leur système de surveillance Echelon au service de l'espionnage industriel au profit des entreprises américaines.

Cette attitude va à l'encontre de tous les principes que les organisations internationales relatives au commerce tentent de promouvoir, et dont les Etats-Unis, principaux bénéficiaires du renseignement, sont membres.

Le droit du commerce international est parfois qualifié de soft law, c'est à dire de « droit mou ». C'est un droit non-contraignant, qui est basé sur la bonne foi des parties contractantes. S'il n'existe pas d'obligation de résultat, il existe néanmoins une obligation de comportement[94]. Conformément à l'accord GATT et aux pratiques de l'Organisation mondiale du Commerce qui en résulte, les Etats se doivent en effet respect et doivent assurer une certaine transparence ainsi qu'une certaine loyauté dans leurs relations commerciales. On peut légitimement s'interroger sur l'existence de la loyauté entre Etats lorsque certains détournent des marchés à leur profit au moyen d'un système d'écoutes secrètes et généralisées.

En outre, l'article 14 de l'accord OMC du 15 avril 1994 stipule que les Etats ne doivent interpréter aucune disposition incompatible avec le respect de la vie privée des personnes

♦ Le rôle ambigu de la Grande Bretagne

S'il apparaît déjà peu louable que des Etats alliés au sein de l'OMC se fasse de la concurrence déloyale à l'aide de techniques d'espionnage, cela l'est encore plus entre des Etats associés dans une organisation telle que l'Union Européenne. C'est pourtant bien ce que suspectent les parlementaires Européens, a propos de la Grande Bretagne.

On sait en effet, depuis les premières révélations sur le système Echelon, que l'Angleterre en est l'un des principaux protagoniste. Or le maintien de la Grande-Bretagne depuis la signature du Traité de Rome au sein d'un pacte Sigint visant le renseignement électronique sous l'égide américaine peut sembler un comble de déloyauté à l'égard de ses partenaires Européens. En effet, L'Union Européenne assure en premier lieu la coopération économique entre les Etats. Mais comment parler de coopération économique lorsque l'Angleterre aide un Etats tiers, les Etats-Unis, à « voler » des marchés économiques aux Européens comme il l'a été montré précédemment ?

[94] Cf. Cours « droit des activités transnationales » de M.Meunier, Université de Lille II. Sur le sujet, voir aussi Prosper Weil, « vers une normativité relative en DIP », RGDIP 1982, p. 5

« Chaque jour, explique David Nataf[95], les deux pays se concertent, tout fonctionne comme un unique et vaste système cogéré, des échanges entre les officiers de renseignements ont lieu »[96]. Il existe en effet en Grande-Bretagne un « SUKLO », special UK liaison officer, et aux Etats-Unis un « SUSLO », special US liaison officer, qui sont constamment en relation.

Si la collaboration est nette sur le plan diplomatique, elle l'est aussi sur le plan technique : Duncan Campbell montre que la plus importante base d'espionnage électronique du monde est la station NSA Field station F83 de Menwith Hill, dans le Yorkshire[97]. Important centre des télécommunications britanniques, La base de Menwith Hill comprend plus de 1800 agents…dont 1200 sont américains !

Suite à la multiplication des révélations dans la presse sur le réseau Echelon, et les suspicions de plus en plus fortes des entreprises Européennes d'être « espionnées », le Parlement européen, en 1997, décida d'effectuer un rapport préliminaire. Celui-ci fut effectué par le STOA, Bureau d'Evaluation des Options Techniques et Scientifiques. Dès 1997, M. Alain Pompidou, président du STOA, expliquait : « des entreprises européennes ont déjà fait les frais [d'Echelon], mais comme elles commercent avec les Etats-Unis, elles se taisent »[98].

Suite à ces révélations, en 1998, le STOA a passé quatre nouvelles commandes de rapports sur « le développement des technologies d'espionnage et le risque d'abus des informations économiques ». L'un de ces rapports constitue l'édition originale du livre de Duncan Campbell et est intitulé Interception Capabilities 2000[99] et fut présenté au parlement Européen les 22 et 23 février 2000, lors d'une cession consacrée à la protection des informations et de la vie privée.

Malgré les révélations d'espionnage présentes, comme nous l'avons vu précédemment (Cf. II.A.2.) , le Parlement Européen n'a pas décidé de mettre en œuvre une réelle enquête sur les pratiques en cause dans le système Echelon.

De toute façon, la délégation de parlementaires européens qui s'est envolée pour les Etats-Unis le 8 mai 2001 n'a pas pu être reçue par les autorités américaines[100].

En France également, les réactions aux révélations sur Echelon n'ont pas manqué. A leur suite, le 29 février 2000, la commission de la défense nationale et des forces armées de l'Assemblée nationale a diligenté une mission d'information. Dont le rôle est d' enquêter sur « les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale ».

---

[95] David Nataf est l'un des avocats qui soutien la plainte du collectif Attawa contre le système Echelon devant le TGI de Paris
[96] David Nataf, Espionnage électronique de l'Europe, Expertises mai 1998.
[97] Echelon et ses alliés, par Duncan Campbell, ZD net, 30 juin 2000
[98] Cité par Philippe Rivière, Le système Echelon, manières de voir n°46, Juillet/ Août 1999
[99] La version originale de ce rapport est disponible en format PDF sur le site http://www.europarl.eu.int/dg4/stoa/en/public/pdf/98-14-01-2en.pdf
[100] Voir Eric Mugneret, Echelon : la NSA pose un lapin à l'Europe, transfert.net, 11 mai 2001

Arthur Paecht, député du Var, qui en est le rapporteur, a remis son rapport au bureau de l'Assemblée le 11 octobre dernier. N'ayant pas le statut de commission d'enquête, la mission a rencontré un certain nombre d'obstacles.

A l'étranger, comme les parlementaires européens, elle s'est heurtée à une fin de non-recevoir de la part des autorités américaines et britanniques.

Ces obstacles n'empêchent pas le rapporteur de conclure à l'existence d'Echelon et de confirmer ses capacités. Suite à ses découvertes, la commission de défense a déposé une proposition de loi visant à créer une délégation parlementaire aux affaires de renseignement. Cette proposition n'a pas encore été inscrite à l'ordre du jour de l'Assemblée Nationale.

Conclusion

Comme nous l'avons souligné, l'essor de la toile n'a pas échappé aux techniciens développant leurs systèmes d'écoutes.

Alors que se développent les moyens d'espionnage électronique, la cryptographie apparaît comme un moyen essentiel pour protéger la confidentialité des échanges et la protection de la vie privée.

Si le réseau Echelon n'est pas nommément cité, la référence y est limpide : d'une phrase, à l'issue du Comité Interministériel pour la société de l'information (CISI) du 19 janvier 1999, Lionel Jospin a redéfini la doctrine française en matière de cryptologie. Cette technique permet de chiffrer et de déchiffrer des messages afin de garantir leur confidentialité et leur intégrité et d'authentifier leur auteur, fonctions indispensables au déploiement de la « net-économie ».

La France s'était jusqu'alors efforcée de limiter la diffusion de ces méthodes, longtemps réservées aux services de renseignement, aux diplomates et aux militaires. Arguant que leur utilisation par le grand public favoriserait la délinquance mafieuse et le terrorisme, les autorités avaient institué un arsenal juridique, unique au monde, destiné à contrôler l'usage des moyens de cryptage et à permettre la récupération des clés secrètes, qui auraient dû être remises à des tiers de confiance, susceptibles de les livrer en cas de besoin à justice.

Mais le gouvernement a fini par reconnaître qu'une telle « ligne Maginot » législative n'était plus adaptée et que la France risquait de se priver d'un moyen de défense vis-à-vis des « grandes oreilles » étrangères, sans en tirer de bénéfice réel.

M. Jospin a donc annoncé la libéralisation du cryptage « de très haute sécurité » utilisant des clés jusqu'à 128 bits, contre 40 bits auparavant. Parallèlement, il fut décidé de renforcer « significativement » les capacités techniques des pouvoirs publics en matière de décryptage et d'écoute.

Enfin, le gouvernement a annoncé une loi rendant obligatoire la remise aux autorités judiciaires, lorsque celles-ci le demandent des transcriptions en clair des textes chiffrés.

Outre le problème qui se pose en matière de crytographie et la question de la protection des données échangées, nous avons pu noter que la grande majorité des interceptions s'effectuent en dehors de l'espace territorial.

Dès lors quelles sont les solutions qui se présentent à l'Etat pour préserver sa souveraineté et ses compétences et quelles évolutions du Droit International Public doivent avoir lieu pour l'y aider ?

En fait, la possibilité qui s'offre à nous est de retenir la notion de souveraineté territoriale en termes fonctionnels et non en termes d'espace.

En effet, certaines activités, parce qu'incoercibles, ne peuvent relever de l'activité des gouvernements de chaque Etat mais d'un seul Etat à raison de la nature de l'activité en cause :

Ceci induirait donc d'effectuer une nouvelle approche du droit international public « à raison des activités et, en matière de cyberespace, de délimiter le champ des interceptions légalement admissibles.

Mais, ceci reste possible uniquement qu'avec le renforcement de la collaboration internationale, voire des Etats-Unis, ce qui semble loin d'être acquis.

BIBLIOGRAPHIE

OUVRAGES

Duncan Campbell, *Surveillance électronique Planétaire*, Editions Allia, 2001

Philippe Oberson, *l'Internet et l'intelligence économique*, Les éditions d'organisation, 1997

François David, *Les échanges commerciaux dans la nouvelle économie mondiale*, PUF, 1994

A. Valladao, *Le XXIème siècle sera américain, La découverte, Paris, 1993*

Nguyen Quoc Dinh, *Droit International Public*, LGDJ, 6ème édition

ARTICLES DE PRESSE

- **PRESSE JURIDIQUE**

Louise Cadoux et Pierre Tabatoni, Internet et la protection de la vie privée, revue Commentaires n°89 (Volume XXIII – 2000)

D. Yernault, Echelon et l'Europe : la protection de la vie privée face à l'espionnage des télécommunications, Journal des tribunaux de droit européen n°72, 1er octobre 2000

Yves Poulet, Le Safe harbor, une protection adéquate ?, texte présenté lors du colloque de l'ICLA, paris 15/16 juin 2000 (juriscom.net, 17 juin 2000)

Claudine Guerrier, Les interceptions de télécommunication, l'Union Européenne et les nouvelles technologies, Petites Affiches n°115, 9 juin 2000

David Nataf, Espionnage électronique de l'Europe, Expertises, mai 1998

Marcel Merle, Un système international sans territoire ?, http://www.conflits.org/Numeros/20merle.html

Cyberespace et Droit International : pour un nouveau Jus Communicationis, Jean-Jacques Lavenue, http://www2.univ-lille2.fr/droit/enseignements/dess_cyber/index.html

- **PRESSE GENERALE**

Michel Ktitareff, « Web bug », un virus à la solde des sites marchands, Les Echos.net, 30 avril 2001

Stéphane Mandard, Echelon face à la vigilance des citoyens, Le Monde, 1er novembre 2000

François Sergent, La fringale du FBI inquiète les américains, Libération des 22/23 octobre 2000.

Jacques Isnard, L'Europe "piégée" par le réseau anglo-saxon d'espionnage Echelon, Le Monde du 13 octobre 2000

Joël Auster, Le FBI nous prend pour des naï fs, Libération, 08 octobre 2000

Echelon, l'espion anglo-saxon espionné, Libération, 05 juillet 2000

Gerard Briard, Echelon: la start up mondiale de l'espionnage, Charlie Hebdo du 24 mai 2000

Philippe Rivière, Contre la corruption étatique, l'espionnage libéral, Ornitho, mai 2000

Philippe Rivière, Petits débats sur Echelon, Le monde diplomatique, 18 avril 2000

R. James Woosley, Pourquoi l'Amérique espionne ses alliés, Le monde diplomatique, avril 2000

Jacques Isnard, La CIA et la NSA justifient des mission du réseau Echelon, Le Monde du 10 mars 2000

La fausse surprise d'échelon, Courrier International, 02 mars 2000

Laurent Zeca, Comment les EU espionnent l'Europe, Le Monde du 23 février 2000

Michel Albertini et Hervé Morin, L'espionnage s'adapte aux nouvelles technologies, Le Monde du 23 février 2000

Philippe Rivière, le système Echelon , Manières de voir n° 46, juillet/aout-99

Le système Echelon, Philipe Rivière, Le Monde Diplomatique http://www.monde-diplomatique.fr/mav/46/RIVIERE/m1.html

Paul Virilio, télésurveillance globale, Le monde diplomatique, juillet 1999
http://www.monde-diplomatique.fr/1999/08/VIRILIO/12332.html

Philippe Rivière, Grandes oreilles américaines, Le monde diplomatique, mars 1999

Philippe Rivière, Tous les européens sur écoute, Le monde diplomatique, mars 1999

Dossier Echelon - les plus grandes oreilles du monde, Courrier International, 02 avril 1998

- **PRESSE SPECIALISEE DANS L'INTERNET**

Marc-Olivier Peyer, **Le FBI mange-t-il les internautes américains tout cru ?,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061424,00.html

Guillaume Bonjean, **La CIA achète son anonymat sur internet de se trouver un bon client**

Jerome Thorel, **Échelon existe, mais pas son antidote,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061429,00.html

Le cybercrime au menu d'un futur forum européen,
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062771,00.html

Jerome Thorel , **Cybercrime : Bruxelles met son grain de sel,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062219,00.html

Guillaume Bonjean, **Cybercrime : le G8 loin du consensus,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061531,00.html

***Jerome Thorel*,** Le cybercrime : nouvelle menace et vieilles recettes,
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060310,00.html

Jerome Thorel, **L'internet sur écoute au Royaume-Uni,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060317,00.html

Jerome Thorel, **G8 : une conférence sur le cybercrime à huis clos,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060402,00.html

Jerome Thorel , **Londres coincé par son projet de surveillance de l'internet,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060820,00.html

Marjorie Sylvain, **Les 15 unis contre la cyber-criminalité,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060953,00.html

Jerome Thore, **Le traité cybercrime met son nez dans les écoutes,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061424,00.html

Jerome Thorel, **Traité cybercrime : les ONG font de la résistance,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061474,00.html

Claire Dubois, **L'Inde adopte des lois contre le cybercrime,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061591,00.html

Jerome Thorel, **Le traité cybercrime modifié,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061643,00.html

Jerome Thorel, **Traité cybercrime : les ONG font de la résistance,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061643,00.html

IRIS, Cybercriminalité : du danger d'un projet de « traité fourre-tout »,
http://www.iris.sgdg.org/actions/cybercrime/analyse-0201.html

IRIS, Communication de la Commission européenne : « créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité »,
http://www.iris.sgdg.org/actions/cybercrime/iris-ec0201.html

Sylvain Simoneau, **Carnivore, l'outil espion du FBI, révolte les Américains,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060848,00.html

Thierry Guilbert, **Carnivore et la NSA, sacrés big brothers américains de l'année,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062534,00.html

Sylvain Simoneau, **Le feuilleton Carnivore traîne en longueur,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061059,00.html

Jerome Thorel, **Carnivore : le FBI transparent sans le vouloir,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061338,00.html

Jerome Thorel, **Le traité cybercrime met son nez dans les écoutes,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061424,00.html

Jerome Thorel, **Des démocrates russes contre le téléflicage de l'ex-KGB,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061309,00.html

Estelle Dumout, **Un forum secret sur les serveurs de la CIA,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061645,00.html

Jerome Thorel, **FBI et Carnivore : ayez confiance,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061716,00.html

Cédric Ingrand, **Écoutes : Carnivore craint l'indépendance des experts,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061215,00.html

Joel Legendre, **Kari-no-mail, un Carnivore à la japonaise,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061825,00.html

Estelle Dumout, **Les internautes polonais bientôt sur écoute,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061934,00.html

Estelle Dumout, **Allemagne : polémique sur la protection des données privées,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062010,00.html

Jerome Thorel, **Clinton soigne son bilan anti-hacking,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062016,00.html

Erich Luening et Jerome Thorel, **Surveillance : le FBI rebaptise Carnivore,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062348,00.html

Guillaume Bonjean, **La Hollande, l'autre pays du flicage,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062401,00.html

Jerome Thorel, **L'Intérieur britannique avide d'écoutes en tout genre,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061798,00.html

A. Pille et J. Thorel, **Plus de moyens pour les cyber bobbies,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061663,00.html

Jerome Thorel , **L'internet préoccupe le contrôleur des écoutes légales,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060592,00.html

Guillaume Bonjean, **Le FBI s'empêtre dans les alertes de sécurité,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2062586,00.html

Christophe Guillemin, **Le système britannique d'écoute des mails obsolète,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060973,00.html

Christophe Guillemin, **La Grande-Bretagne autorise l'écoute des mails,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060945,00.html

Jerome Thorel, **Internet : la loi « liberticide » de Tony Blair passe le cap des Lords,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060876,00.html

Sylvain Simoneau, **Rip Bill : le Royaume-Uni obligé de s'aligner sur l'Europe,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2061110,00.html

Jerome Thorel, **Londres coincé par son projet de surveillance de l'internet.**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060820,00.html

Jerome Thorel, **Un ministre coincé pour délit électronique,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2058852,00.html

Jerome Thorel, **Les réseaux européens sur écoute,**
http://news.zdnet.fr/zdnetfr/news/story/0,,s2060676,00.html

La cyber-guerre à l'orée du XXIe siècle,
http://www.confidentiel-defense.com/mag/informat/cybergue.htm

Comment la NSA espionne le Monde,
http://www.confidentiel-defense.com/anciens/numero%201/nsa.htm

Jean-Marc Manach **Cybersurveillance : la crypto inutile ?,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=5531

Benjamin Cherrière, **SilentRunner : le renifleur,**
http://www.transfert.net/fr/techno/article.cfm?idx_rub=89&idx_art=4503

Jean-Marc Manach, **Carnivore, Big Brother toutes catégories,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=4616

Jean-Marc Manach, **Les Américains n'ont pas confiance en leur gouvernement…,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=5009

Edgar Pansu, **La Maison Blanche s'intéresse à la vie privée,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=5325

Matthieu Auzanneau, **Toutes les taupes n'utilisent pas de souris,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=4247

François Landon, **Avec Technosphere, on est tous des Dieux,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=4223

Jean-Marc Manach, **Ne m'appelez plus jamais Carnivore,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=4175

Matthieu Auzanneau, **:-(est une marque déposée,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=3817

Jean-Marc Manach , **La crème des atteintes à la vie privée,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=3451

Jean-Marc Manach, **Le Carnivore se met au sushi,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=2746

Karine Portrait, **Big Brother parle aussi polonais,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=3225

Arnaud Gonzague, **Carnivore est doux comme un agneau !,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=2672

Matthieu Auzanneau, **Surfer comme des bêtes,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=2524

Antoine Champagne, **Cyber-criminalité : l'Europe dégaine l'arsenal répressif,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=2156

Jean-Marc Manach , **Carnivore est plus méchant que prévu,**
http://www.transfert.net/fr/revue_web/article.cfm?idx_rub=94&idx_art=2126

Jean-Marc Manach , **Un Carnivore dans leurs ordis,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1203

Jean-Marc Manach, **Carnivore : la Maison Blanche veut légiférer,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1220

Jean-Marc Manach, **Carnivore bientôt open source ?,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1304

Christophe Agnus, **Coup de frein pour le Carnivore téléphonique,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1428

Arnaud Gonzague, **3 000 pages d'infos sur Carnivore…,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1443

Matthieu Auzanneau , **La Justice américaine enquête sur Carnivore,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1532

Arnaud Gonzague, **Un Carnivore pour tous les fournisseurs d'accès,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1859

Carnivore FAQ (Frequently Asked Questions),
http://www.robertgraham.com/pubs/carnivore-faq.html

Karen Bastien , **Carnivore a trouvé son groupe d'experts,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1900

Karen Bastien, **La Justice américaine prise à son propre piège,**
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=1928

Jean-Marc Manach, **Les Carnivores du FBI,**
http://www.transfert.net/fr/revue_web/article.cfm?idx_rub=94&idx_art=1183

Echelon : **la NSA pose un lapin à l´Europe**, Eric Mugneret, transfert.net,
http://www.transfert.net/fr/cyber_societe/article.cfm?idx_rub=87&idx_art=5579

« **je n'attends pas grand-chose des auditions sur Echelon** », Alain Krivine porte parole de la LCR et eurodéputé,
http://transfert.net/fr/cyber_societe/article.cfrn?idx_rab=87&idx_art=5530

Ph. Crouzillac, **Protection des données personnelles, Washington menace le Safe Habo**r, 01 net, 29 mars 2001

Jean Marc Manach**, Ne m'appelez plus jamais Carnivore**, Transfert.net, 16 février 2001

Yahoo! Actualités, **USA: les experts favorables au système d'espionnage Carnivore**, 15 décembre 2000

Jean Marc Manach, **Carnivore plus méchant que prévu**, Transfert.net, 16 octobre 2000

Jean Marc Manach, **L'Europe enquête sur Echelon à reculons**, Transfert.net, 06 juillet 2000
http://transfert.net/fr/cyber_societe/article.cfrn?idx_rab=87&idx_art=1141

Jean Marc Manach, **La France et l'Europe se penchent sur Echelon**,
Transfert.net, 05 juillet 2000

Jean Marc Manach, **Echelon mis à nu**, Transfert.net, 31 janvier 2001-05-21

Jean Marc Manach, **Echelon au rapport**, Transfert.net, 17 octobre 2000

Jean Marc Manach, **Echelon is watching you**, Transfert.net, 05 juillet 2000

Eric Mugneret, Echelon, **la NSA pose un lapin à l'Europe**, Transfert.net, 11 mai 2001

Duncan Campbell, **Echelon et ses réalités**, ZD Net, 30 juin 2000

Danielle Kaminsky et Jérôme Thorel, **Frenchelon, les grandes oreilles made in France** ZD Net, 21 juin 2000

Cédric Ingrand et Joël Legendre**, Echelon et ses alliés....parfois officieux**, ZD Net, 21 juin 2000

COMMUNIQUES

EPIC Press, FBI Releases Carnivore Documents to EPIC Privacy Group Says Disclosure Insufficient, 02 octobre 2000

Philippe COUVE, *Réseau Echelon : la justice française ouvre une enquête*; http://www.fas.org/irp/program/process/echelon.htm

Comment la NSA espionne le monde ; Confidentiel - Défense - juillet 2000 - http://www.confidentiel-defense.com

Trois question àDuncan Campbell, http://cdcp.free.fr/dossiers/echelon/dc.htm, *Interview pour Radio France International*

Compte rendu de l'audition de Monsieur Yves Poullet, le 11 octobre 2000 devant le groupe de travail "Société de l'information" du parlement belge, www.droit.fundp.ac.be/Textes/CCE.pdf