EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT

STOA

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

Vol 1/5

Présentation et analyse

1) Présentation des quatres études
2) Analyse: protection des données et Droit de l'Homme dans l'Union Européenne et rôle du Parlement Européen

Document de travail pour le Panel STOA

Luxembourg, Octobre 1999 PE 168.184/Vol 1/5

Cataloguing data:

Title:	**Vol 1/5: Présentation et analyse** **1) Présentation des quatre études** **2) Analyse: protection des données et Droit de l'Homme dans l'Union Européenne et rôle du Parlement Européen**
Workplan Ref.:	EP/IV/B/STOA/98/1401
Publisher:	European Parliament Directorate General for Research Directorate A The STOA Programme
Author:	Peggy Becker - visiting researcher Sous la direction de Dick Holdsworth, chef de l'unité STOA
Editor:	Mr Dick HOLDSWORTH, Head of STOA Unit
Date:	Octobre 1999
PE number:	PE 168. 184 Vol 1/5

Ce document fait partie d'une série publiée en cinq volumes (Vols. 1/5 - 5/5).
Les différents volumes sont publiés en langue originelle.
Une version complète en anglais et français sera publiée ultérieurement.

Table des matières :

Introduction…… 4

Première partie : Présentation des quatre études

1) Le premier document : « The state of art in communication intelligence(…) »……6

2) Le deuxième document : « Chiffrement, cryptosystème et surveillance électronique : un survol des technologies » ……. 8

3) Le troisième document : « The legality of interception of electronic communication : a concise survey of principal legal issues(…) » ……10

4) Le quatrième document : « The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception »……..…11

Deuxième partie : Analyse: Protection des données et Droits de l'Homme dans l'Union européenne et rôle du Parlement européen

1) Les Droits de l'Homme et l'Europe :

A. Les Droits de l'Homme et l'Union européenne…… 13
B. Les Droits de l'Homme et le Parlement européen…… 14
C. La place du respect de la vie privée dans la protection européenne des Droits de l'Homme…… 16

2) Surveillance électronique et réglementation :

A. Les interceptions légales :
1. Réglementation communautaire et la position du Parlement……17
2. L'application dans les Etats membres…… 21
B. Les interceptions globales :
1. Description…… 23
2. Les risques possibles…… 24
3. La position de L'Union européenne et du Parlement…… 25

3) Cryptographie et chiffrement : la clef du problème ?

A. Présentation et problématique…… 26
B. La position de l'Union européenne…… 27
C. Position divergente d'Etat membre : le cas de la France…… 29

Conclusion ……. 31
Annexe :définitions et résolution B4-0803/98 …… 32
Bibliographie…….. 34

INTRODUCTION

L'expression *«vie privée »* d'un usage relativement récent recouvre une réalité aussi ancienne que la volonté des personnes d'être à l'abri des pouvoirs de l'autre. En effet, la vie privée est la sphère d'existence intime de l'individu ainsi elle doit être soustraite à la connaissance d'autrui et protégé de leur curiosité.

Le droit au respect de la vie privée s'inscrit dans les droits de la personnalité reconnus assez récemment. L'article 8 paragraphe 1 de la Convention Européenne des Droits de l'Homme[1] (CEDH) garantit le respect de ce droit : « Toute personne a droit au respect de sa vie privée et familiale de son domicile et de sa correspondance ». Cette convention s'inscrit dans un ensemble d'actes juridiques internationaux et nationaux reconnaissant ce principe protecteur. Mais la *vie privée* n'a jamais été réellement définie, elle comprend le droit à l'intimité, le droit au secret de sa correspondance y compris téléphonique et électronique et la protection contre l'informatique et le traitement des données à caractère personnel. Ce droit a donc d'abord été protégé par des dispositions ponctuelles :- inviolabilité du domicile, des correspondances et du secret professionnel ; puis avec la naissance d'agressions, de viols plus modernes : - interceptions électroniques ; écoutes téléphoniques ; enregistrement etc…la vie privée a fait l'objet de disposition protectrice générale car les atteintes n'ont en fait cessé d'augmenter dans notre décennie. C'est ainsi qu'a été conclue à Strasbourg le 28 janvier 1981 la convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, elle est entrée en vigueur le 1er octobre 1985.Celle-ci ne contient pas de règles directement applicables dans l'ordre interne des Etats membres mais se borne à énoncer les principes protecteurs de la vie privée que les états s'engagent à mettre en œuvre, tous les états ayant déposés leur instrument de ratification ont dû préalablement adopter une législation en accord avec les principes qui y sont contenus.

La protection de la vie privée est donc bel et bien ancrée dans les systèmes juridiques nationaux et internationaux comme dans celui communautaire. Bien qu'ainsi affirmé on pourrait penser que ce droit est intouchable, mais il faut pourtant ajouter qu'une conciliation est nécessaire avec les besoins de sécurité, défense nationale ou de lutte contre le terrorisme. C'est pour répondre à ces besoins qu'il existe certaines entraves autorisées comme les interceptions légales de communication qui peuvent être mises en œuvre, mais seulement celles-ci car elles bénéficient d'une réglementation stricte dont les lignes directrices ont été avancées par l'Union européenne puis suivies par les Etats membres. Outre ces ‘‘interceptions légales’’, l'Union européenne qui se doit de suivre la CEDH et les autres conventions va devoir lutter contre les interceptions illégales, mais aussi contre celles légales qui sont détournées de leur but premier et avec le développement de nouvelles technologies ces dernières deviennent d'une application simple.

---

1. Le texte définitif de cette convention fût signé à Rome le 04 novembre 1950 mais sa ratification par les états pris plus de temps, en septembre 1997 tous les états membres l'ont ratifié.

En effet, les moyens de communication modernes (fax, mobile, internet…) engendrent certains risques concernant la confidentialité des correspondances et notamment dans les domaines économiques où l'utilisation de ces derniers est de plus en plus courante comme pour les activités commerciales.

De plus, dans un même temps il s'est développé une très vaste gamme de techniques de surveillance ; microphone parabolique, la version laser…Celles-ci peuvent être définies comme des dispositifs ou des systèmes capables de surveiller, de suivre et d'évaluer les mouvements des personnes, de leurs biens ou avoirs. Ces nouvelles formes de surveillance apparues ont consisté à automatiser l'interception des communications. Les conséquences de ces interceptions peuvent être importantes notamment du point de vue économique. On remarque donc qu'il s'agit là d'un domaine du progrès technique dans lequel les réglementations d'un autre âge sont dépassées par des interceptions nouvelles qui sont en augmentation constante et qui ne peuvent être encore considérées comme des infractions.

Pour remédier à cela, l'Union européenne et plus précisément le Parlement européen à mis en œuvre une action commune. C'est ainsi que la commission des Libertés Publiques et des Affaires Intérieures[1] a demandé à la STOA (Scientific and Technological Option Assessment) d'établir une étude à ce sujet. Ce document a pour but de vous présenter cette étude qui est composée de quatre rapports qui établissent un inventaire des nouvelles technologies de télécommunication, de leurs risques et des moyens à développer pour enrayer ces derniers.

Pour bien comprendre l'ensemble de la question nous allons présenter succinctement les quatre documents pour ensuite en faire une analyse, celle-ci portera sur les interceptions légales et la législation en vigueur ainsi que les interceptions globales de communication, et la cryptographie qui est peut-être la solution au problème de la confidentialité.

---

1. Depuis juillet 1999 cette commission est dénommée : la Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures -LIBE

Première partie :

PRESENTATION DES QUATRE ETUDES

INTRODUCTION :

A la demande de la Commission des Libertés Publiques et des Affaires Intérieures[1] la STOA a mis en œuvre une étude intitulée «DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION ». Cette étude est la suite logique du rapport[2] publié en septembre 1998 par la STOA sur l'« EVALUATION DES TECHNIQUES DU CONTROLE POLITIQUE » rédigé par la fondation OMEGA à Manchester. Ce document a trait à la question spécifique de la surveillance électronique, il évoque donc les récents progrès réalisés en la matière, il résume les tendances des réglementations actuelles en Europe et dans les pays tiers. Il présente aussi une série d'option comme la commande d'étude plus détaillée sur les incidences sociales, politiques, commerciales et constitutionnelles des réseaux globaux de surveillance électronique qu'il a cité, en vue d'organiser une série d'audition d'experts afin d'étayer la future politique de l'Union Européenne en matière de liberté publique.

Les quatre rapports qui seront présentés ici, répondent tout à fait à cette demande. En effet il s'agit bien d'une étude concernant l'impact de la surveillance électronique dans l'Union Européenne qui va permettre aux institutions et notamment aux membres du Parlement Européen de comprendre et de connaître l'état actuel des moyens et de l'utilisation de la surveillance électronique pour leur permettre ainsi d'avoir tous les renseignements nécessaires pour mettre en place une réglementation plus soucieuse du respect de la confidentialité des communications et aussi éliminer au maximum les risques économiques que ces interceptions et que la libre concurrence peuvent engendrer.

1) **Le premier document : « The state of art in Communications Intelligence (COMINT) of automated processing for inteligence purposes of intercepting broadband multi-language leased or common carrier system, and its applicability to COMINT targeting and selection, including speech recognition. »[3]**

Ce document rédigé par Duncan Campbell[4] pour la Direction Générale des Etudes du Parlement européen et plus précisément pour la STOA met en évidence l'état actuel de la surveillance électronique via *THE COMMUNICATIONS INTELLIGENCE : COMINT* c'est-à-dire la recherche de communication électronique qui permet l'interception globale de celle-ci. Elle est définie par la NSA comme une activité industrielle qui permet d'intercepter toutes communications étrangères. [5]

---

1. Depuis juillet 1999 cette commission est dénommée : la Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures.
2. Le projet de la STOA « UNE EVALUATION DES TECHNIQUES DE CONTROLE POLITIQUE » a fait l'objet d'une étude intérimaire rédigé par OMEGA :PE 166.499
3. STOA PE 168.184/part4/4 avril 1999
4. Duncan CAMPBELL IPTV Ltd Edinburgh SCOTLAND *mailto :iptv@cwcom.net*
5. NSA : NATIONAL SECURITY AGENCY. La définition a été donnée lors du conseil de la sécurité nationale des Etats-Unis le 17 février 1972 dans la directive N°6.

En effet, il évoque les nouvelles technologies utilisées en expliquant de quelles manières et par quelles méthodes elles travaillent et pour mieux comprendre ces systèmes il attire notre attention sur les cibles visées par les interceptions globales. Ces nouveaux systèmes facilitent la surveillance de masse de toutes les télécommunications. Il faut préciser aussi que sans encodage les moyens modernes de communication sont transparents face aux équipements de pointe en matière d'interception qui peuvent être utilisés pour les écoutes téléphoniques par exemple. Ce rapport montre donc que depuis la naissance de la recherche électronique de communication il y a eu une véritable évolution dans les moyens d'interception(1) et ces derniers sont de plus en plus sophistiqués (les ressources utilisées sont proportionnelles aux fins souhaitées : 15- 20 billion d'euros).

La recherche électronique de communication, étant sur une large échelle une activité industrielle la plus part des nations l'utilise mais la plus importante est l'organisation *UKUSA*(2) des nations anglophones. Ce document met aussi en évidence de nouvelles informations sur le système *ECHELON*(3) qui fait partie du système anglo-américain, il permet une surveillance du monde entier et à l'inverse de beaucoup d'autres il vise essentiellement des cibles non militaires. Il fonctionne en interceptant de très grandes quantités d'informations puis en triant les éléments à l'aide de système d'intelligence artificielle.

Toutes ces organisations étant mises en place, les différents états les composants ont dû prendre certaines mesures pour les réglementer, les surveiller. Cette étude reprend l'historique des différentes réglementations mises en application et il montre bien la prédominance des Etats-Unis, qui au début grâce à l'influence du FBI ont organisé un rassemblement d'états(4) pour discuter ensemble des différentes législations possibles. La position des Etats-Unis y est décrite. Selon l'auteur, celle-ci ne va pas réellement dans un sens propice au respect de la confidentialité et donc de la vie privée, en effet la politique de la *NSA* (NATIONAL SECURITY AGENCY) tendrait plutôt à faire tout pour faciliter les interceptions. Ils justifient leur point de vue par certains exemples comme la lutte contre la criminalité, le terrorisme et ils l'expliquent aux autres pays pour que ces derniers se joignent à cette politique. La réaction de l'Union européenne et des pays de l'*OCDE* est aussi dépeinte dans ce rapport. Elle peut se résumer (pour l'Union) à une résolution du Conseil prise en janvier 1995 et qui suit en fait à peu de choses près les idées américaines (mais certains états membres réussissent tout de même à faire de la résistance).

La question reste bien sur de savoir pourquoi l'intérêt des américains est si grand. La réponse qui est donnée par l'auteur, est tout simplement liée au système *ECHELON* qui permet aux nations l'utilisant d'obtenir certaines informations primordiales sur le plan économique et ainsi avoir une position des plus intéressante sur les marchés commerciaux. Et cela n'est pas sans avoir des conséquences importantes, en effet des exemples sont donnés, dans cette étude, où des marchés, des contrats ont pu être obtenus par des compagnies américaines grâce à l'interception de communications. Peut-on penser que pour vaincre la concurrence tout peut être bon ?

---

1. Voir rapport de la page 3 à 13.
2. UKUSA date d'un accord entre le Royaume-Uni et les Etats-Unis sur les interceptions électroniques, les nations de l'alliance UKUSA sont les Etats-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.
3. Le système ECHELON existe depuis les années 1970.(et c'est considérablement développé entre 1975 et 1995)
4. Ces rencontres se nomment ILETS : INTERNATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SEMINAR, elles ont été initiées et fondées par le FBI depuis 1993.

Les nouvelles technologies développées à la fin de ce siècle ont donc permis à la *COMINT* d'avoir d'énormes capacités d'interception mais l'arrivée de l'an 2000 va certainement bouleverser cet état de fait. Car le progrès technique et le changement des mentalités vont permettre au chiffrement et à la cryptographie d'être réellement intégrés dans les télécommunications.

Mais, des mesures doivent tout de même être prises par l'Union Européenne et plus précisément par le Parlement qui a été trop longtemps laissé à l'écart des discussions sur ce sujet. Le rapport dont il est question évoque quelques politiques possibles que devrait suivre le Parlement et qui permettraient à l'Union Européenne de se dégager de l'influence des Etats-Unis.

Le respect de la confidentialité des communications est donc loin d'être total et cela engendre des inégalités profondes sur le plan économique entre les différents pays qui sont plus ou moins attachés à ce principe dans leur législation et s'ils le respectent, ils peuvent se voir mis à l'écart lors de passation de marchés importants par un pays qui utilise le système de recherche électronique de communication. Le problème pourrait être résolu par la généralisation des moyens de cryptage et de chiffrement. Le deuxième dossier traite de ce sujet et nous permet d'avoir des renseignements utiles sur ces systèmes.

2) Le deuxième document : « Chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie[1] »

Le but de ce rapport est de décrire les principales techniques qui permettent de se préserver contre toutes formes d'interception technologique de communications. Il a été rédigé par le Dr Franck Leprévot[2].

Cette étude reprend les différents types de technologies qui sont apparus en matière de télécommunications et leurs risques[3], puis établit une explication des techniques de cryptographie et de chiffrement, car la surveillance électronique qui permet bien souvent de protéger la sécurité nationale connaît aussi certains effets pervers comme l'espionnage industriel. Le Dr Leprévot met donc en avant les différents moyens qui permettent la sécurité des communications (chiffrement, cryptographie), mais il expose aussi les conséquences de la cryptanalyse, qui est la mise au point de techniques ou d'attaques pour réduire la sécurité théorique d'algorithmes cryptographiques et de la cryptanalyse quantique, qui est l'ensemble des techniques permettant de trouver les clefs secrètes de protocoles cryptographiques à l'aide d'ordinateurs quantiques. Il est donc vrai que le respect de la confidentialité des communications et du secret de la correspondance peut-être protégé, mais cette protection est loin d'être totale.

Le problème des interceptions de communications se pose toujours même si l'utilisateur émettant utilise des méthodes de codage les plus sophistiquées. De plus les institutions européennes sur les traces des Etats-Unis travaillent pour mettre au point un coprocesseur quantique qui rendrait la cryptographie à clef publique (définie et expliquée dans le rapport) obsolète.

---

1. STOA PE 168.184/Part ¾ : avril 1999
2. Dr Leprevot est professeur à l'université technique de Berlin (TUB)
3. Voir pages 2 et 3 du rapport

On peut donc relever, selon les affirmations de l'auteur, que d'une part l'Union européenne prône les droits fondamentaux et d'autre part travaille, en quelque sorte, en leur encontre.

Les conséquences politiques, diplomatiques et financières de la cryptanalyse et de la cryptographie quantique peuvent être très importantes, c'est pour cela que les différents pays ont signé plusieurs accords pour contrôler ces procédés. Le dernier en date est l'accord de WASSENAAR[1], le document du Dr Leprévot commente sa partie : *SECURITE DE L'INFORMATION* et met en avant les conséquences de ce dernier.

L'accord de WASSENAAR identifie un régime international de contrôle à l'exportation des armes conventionnelles et des biens et technologies à double usage, ainsi qu'une liste de ces éléments. La cryptographie fait partie de cette liste. Cet accord remplace l'accord du COCOM. Il contrôle l'exportation des procédés de cryptographie en tant que bien à double usage, c'est à dire à la fois des applications civiles et militaires. Mais cet accord stipule aussi que les produits clairement identifiés et vendus à des fins civiles ou commerciales ne peuvent faire l'objet de restrictions et de contrôle. En fait, seule les techniques offrant un degré de sécurité très restreint sont autorisées sans contrôle. Tout cela n'est pas sans avoir des conséquences notamment au niveau communautaire. Ce rapport fait une description de ces dernières puis suggère des options possibles aux institutions européennes pour mettre en place une réglementation plus soucieuse du respect de la vie privée. Car les entreprises, organismes ou individus se dotant d'un système cryptographique répondant aux critères légaux peuvent voir leurs communications être interceptées et décodées par le réseau ECHELON. En effet, la cryptographie «légale» ne permet pas de protéger réellement contre les interceptions globales de communications.

Il est donc évident que loin de limiter le crime et le terrorisme, le développement des restrictions sur la cryptographie ne peut que créer un environnement dans lequel le citoyen ne sera pas protégé face au «terrorisme de l'information et aux activités cyber-criminelles» et donc où le crime pourra impunément prospérer, car aucune information ne bénéficiera d'une réelle protection et donc d'une véritable confidentialité.

De grands progrès restent à être réalisés en ce qui concerne l'utilisation de la cryptographie et du chiffrement, par contre, il existe dans tous les pays de l'Union Européenne une réglementation sur les interceptions légales. Leur mise en œuvre est étroitement surveillée et encadrée, c'est ce que nous montre le troisième document que nous allons vous présenter, celui-ci permet aussi de déterminer si ces réglementations sont ou non conventionnelles.

---

1. L'accord de WASSENAAR a été signé le 19 décembre 1995 par 33 pays parmi lesquels la plupart des pays européens ainsi que l'AUSTRALIE, le CANADA, les ETATS-UNIS, le JAPON et la NOUVELLE-ZELANDE.
2. Cf. : http://www.wassenaar.org/

3) Le troisième document : THE LEGALITY OF THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS : A CONCISE SURVEY OF PRINCIPAL LEGAL ISSUES AND INSTRUMENTS UNDER INTERNATIONAL, EUROPEAN AND NATIONAL LAW[1].

Ce rapport a été rédigé par le professeur Chris Elliott, juriste et ingénieur spécialisé dans les télécommunications, il examine les différentes politiques existantes concernant les interceptions légales de communication.

Il a relevé les différentes conventions internationales qui traitent des droits de l'homme et de la protection de la vie privée tout en mettant en avant les portes qu'elles laissent ouvertes à d'éventuelles réglementations «contraires» à ces droits. Par exemple, la Déclaration Universelle des Droits de l'Homme[2] ne dit pas que les interceptions légales sont interdites mais seulement celles réputées arbitraires. De cette manière l'Union européenne a mis en place une législation[3] permettant aux états membres de légaliser certaines interceptions de communications. En effet, l'Union ne va pas à l'encontre de droits proclamés dans les conventions internationales qu'elle a ratifié, en n'interdisant pas les interceptions légales non arbitraires puisque ces dernières ne les interdisent pas elles même.

Les différents états membres ont donc chacun une réglementation sur les interceptions légales qui doit suivre les règles du droit dérivé européen. Ces réglementations sont plus ou moins similaires. Le rapport, dont il est question, expose succinctement les législations nationales existantes sur le problème. Il permet donc d'avoir les éléments principaux sur ces dernières, mais pour savoir si les états membres sont réellement placés dans le même sens que l'Union il faudrait examiner la jurisprudence des instances communautaires (cf. La deuxième partie que nous allons traiter).

Les conventions concernant les droits de l'homme, surtout la CEDH, permettent une protection efficace contre les interceptions illégales de communication. Mais, cette protection est moins évidente contre les interceptions légales et surtout si elles sont étrangères (c'est à dire que l'interceptant est un pays autre que celui de l'émettant). En effet, certains pays ont la capacité d'intercepter une communication interne d'un autre pays. Des mesures doivent être prises pour limiter ce type d'interceptions et l'Union européenne a la possibilité de mettre en œuvre une protection plus efficace de la vie privée, sans pour autant aller à l'encontre des législations nationales mises en place, comme en exigeant par exemple que les réseaux opérateurs permettent une meilleure confidentialité des communications en utilisant le chiffrement. Le professeur Elliot dresse quelques observations et donne quelques exemples que devrait suivre l'Union pour améliorer le respect de la vie privée et de la correspondance.

Cette étude permet donc de connaître la législation en vigueur concernant les interceptions légales de communications.

---

1. STOA PE 168.184/Part2/4 : avril 1999
2. La Déclaration Universelle des droits de l'Homme adoptée par l'Assemblée générale des Nations Unies sous la forme d'une résolution le 10 décembre 1948.
3. La législation de l'Union Européenne : Résolution du conseil du 17 janvier 1995 (1992 JO L123)
   Directive 95/46/EC
   Directive 97/66/EC

4) Le quatrième document : THE PERCEPTION OF ECONOMIC RISKS ARISING FROM THE POTENTIAL VULNERABILITY OF ELECTRONIC COMMERCIAL MEDIA TO INTERCEPTION [1]

Cette étude du développement de la surveillance électronique a été conduite par le cabinet d'études ZEUS (Europeen Economic Interest Grouping), situé à Patras, sous la direction de M. Nikos BOGONIKILOS, à la demande de la STOA et terminée en juin 1999. Son but a été d'examiner l'utilisation d'interceptions légales de communication et de mettre en évidence les risques possibles quant à ces dernières, notamment concernant le commerce électronique.

Elle est organisée en trois parties : les options possibles ; les évidences (avis d'experts) ; un dossier technique sur les nouvelles technologies. Ce rapport est intéressant car il fait appel à l'avis d'experts c'est-à-dire quarante neuf personnes spécialisées dans le secteur des télécommunications et des nouvelles technologies s'y rapportant.

Certaines options politiques y sont proposées comme par exemple la mise en place d'un réseau global pour les communications, la possibilité de définir les capacités d'anonymat qui sont recommandés. Ces dernières ont pu être prises après avoir examiné la consultation des experts, ils sont tous d'accord aujourd'hui pour dire que presque toutes les informations économiques s'échangent par voie électronique. Il faut donc pour être efficace étudier la protection face à l'électronique par rapport à un réseau international et il est crucial d'établir une réelle confidence des communications via les nouvelles technologies. 90% d'entre eux estiment que malgré les différentes législations il existe encore des activités illégales et depuis le développement d'Internet l'augmentation des transactions entraîne un besoin d'établir un encadrement stable pour les relations commerciales, ils pensent aussi que pour assurer une réelle protection de la vie privée il faut définir une réglementation politique et sociale.

Le dossier technique de ce rapport donne quant à lui une vision d'ensemble de la surveillance électronique, car dans cette partie l'auteur définit certains termes techniques et les méthodes d'utilisation comme les interceptions globales (c'est à dire internationales) permises par *COMINT*, la recherche de communication électronique qui est une sorte d'activité industrielle permettant l'interception de ces communications. Une liste non exhaustive des organisations qui utilisent cette recherche est mise en avant dans cette partie, la plus importante étant l'organisation des nations anglophones *UKUSA*.

Il est évident qu'Internet et les autres systèmes de communication modernes sont de plus en plus présent dans la vie de tous les jours. Mais ces derniers sont vulnérables car ils ne permettent pas un véritable respect de la confidentialité. De plus, dans un même temps, des systèmes de surveillance se sont développés tel que les systèmes *CALEA* ou *ECHELON* qui sont définis dans cette étude[3], celui-ci explique aussi le «comment et le pourquoi » d'utilisation de ces systèmes.

---

1. Ce document met en avant les résultats analytiques de l'étude : PE 168.184/Int.St/part1/4
2. STOA PE 168.184/Int.St/part1/4 : mai 1999
3. Voir pages 11 et 12 du rapport en question.

Il semble donc que la nature des informations recueillies par les interceptions n'est pas sans incidence sur les effets et sur le but de tels agissements. Si les interceptions de communication sont effectuées dans le sens d'une volonté de protéger les personnes c'est à dire dans un but de défense nationale ou de lutte contre la criminalité, le terrorisme, moins de problèmes se posent mais si les informations recueillies sont utilisées dans un seul intérêt notamment économique, certains dangers peuvent survenir comme le risque d'abuser de ces informations pour faire gagner à certaines compagnies des marchés commerciaux (espionnage industriel), des exemples d'abus sont donnés par cette étude qui illustrent bien ces dangers[1]. Mais le progrès technique ne va pas seulement dans un sens (permettre que les interceptions soient de plus en plus facile), donc de nouveaux systèmes de protection se sont aussi développés comme le chiffrement ou la cryptographie[2]

Pour comprendre l'ensemble de la question de la surveillance électronique il ne faut pas oublier d'étudier la réglementation en vigueur[3]. Cette étude dresse un historique de celle-ci. L'Europe est le premier lieu où une législation pour la protection de la vie privée à vu le jour, le respect de la confidentialité y est considéré comme un droit fondamental. Il n'en va pas de même partout, en effet aux Etats-Unis cette protection est limitée par des conflits d'intérêts notamment économiques. Ce pays va user de sa prédominance (étant la première puissance mondiale) pour faire accepter et adopter sa position aux autres états :- limiter le chiffrement et le cryptage ; - augmenter les capacités d'interception…C'est ce que cette étude met en évidence. Cependant, l'Union européenne a tout de même su imposer quelques initiatives pour permettre une meilleure protection de la confidentialité et donc des données personnelles.

Cette étude donne une vision d'ensemble de la question de la surveillance électronique, elle permet de comprendre l'intérêt que peuvent avoir certains états à utiliser ces méthodes. Il existe donc bien des interceptions légales de communication, elles sont légales car réglementées par les états.

Ici se termine la présentation des quatre études, les textes originaux de celles-ci sont présentés à la suite de ce document. Mais il faut ajouter que les indications, contenues dans les différents rapports, comme par exemple, la question des interceptions légales et leur réglementation dans les états membres ou encore celle sur la cryptographie, supposent une analyse plus approfondie qui se rapporte à la protection des données et aux Droits de l'Homme dans l'Union européenne. C'est pourquoi, nous allons essayer d'apporter des éléments nouveaux pour mieux répondre à ces questions dans la deuxième partie de cette étude.

---

1. Voir pages 13 à 15 du rapport en question.
2. Cf. STOA PE 168.184/Int.St/part3/4 « Encruption and cryptosystems in electronic surveillance » 1999
3. Voir pages 16 à 21 du rapport en question.

Deuxième partie :

ANALYSES: PROTECTION DES DONNEES ET DROITS DE L'HOMME DANS L'UNION EUROPEENNE ET RÔLE DU PARLEMENT EUROPEEN

INTRODUCTION :

L'histoire de l'humanité est marquée par les différents efforts mis en œuvre pour assurer le respect de la dignité humaine. La notion de Droit de l'Homme a été introduite et développée par des penseurs appartenant à différentes traditions religieuses et culturelles. Des hommes d'état et juristes ont beaucoup contribué au progrès de ces droits et aux normes juridiques s'y référant. C'est ainsi que les droits des individus ont progressivement trouvé leur place dans la législation des différents états.

Le problème qui nous concerne : la surveillance technologique, est au cœur de la question des Droits de l'Homme, car elle touche en effet au respect de la vie privée qui est un droit fondamental reconnu pleinement aujourd'hui. Les rapports que nous avons présentés en première partie nous amènent à faire quelques commentaires concernant notamment : - les Droits de l'Homme et l'Europe ; - les interceptions de communications et la réglementation en vigueur ; - le chiffrement et la cryptographie.

1) Les Droits de l'Homme et L'Europe :

Nous allons ici présenter les Droits de l'Homme dans l'Union européenne d'une manière générale pour ensuite examiner la question plus précisément par rapport à l'une des institutions : le Parlement européen. Il est utile aussi de mettre en évidence la place que prend le respect de la vie privée dans la protection européenne des Droits de l'Homme.

A. Les Droits de l'Homme et l'Union européenne :

Le Conseil de l'Europe à peine mis en place en 1949 que six de ses pays fondateurs[1]décident d'intégrer leur économie dans deux secteurs : le charbon et l'acier[2]. C'est ainsi que de nouvelles institutions communes voient le jour. Un changement radical des relations entre ces états est donc mis en œuvre et entraîne une solidarité de fait entre eux qui sera bientôt concrétisée. Ce premier traité consacre le «droit » avec la mise en place de la Cour Européenne de Justice, mais les Droits de l'Homme dans leur formulation large ne sont pas mentionnés dans ce dernier. Ils ne font pas non plus l'objet d'une référence explicite dans le traité de Rome[3] instituant la communauté économique européenne.

---

1. La République Fédérale d'Allemagne ; la Belgique ; la France ; l'Italie ; le Luxembourg et les Pays-Bas.
2. Le traité de Paris du 18 avril 1951met en place cette intégration.
3. Le traité de Rome fût signé le 25 mars 1957.

Mais, il ne faut pas oublier que le vieux continent a élaboré en 1950 la «Convention Européenne de Droits de l'Homme et des Libertés Fondamentales» qui est la référence en la matière en Europe. De plus il a été mis en place une juridiction de contrôle : la Cour Européenne des Droits de l'Homme siégeant à Strasbourg est chargée de veiller au respect de la convention. Il faut noter cependant que les institutions communautaires ne relèvent pas du contrôle direct de la Cour de Strasbourg.

C'est dans le Traité sur l'Union européenne (article 6) que sont pour la première fois exposés les principes fondamentaux du respect des droits de l'homme : *« l'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et des libertés fondamentales, ainsi que l'état de droit, principes qui sont communs aux états membres. L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la CEDH, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles communes aux états membres, en tant que principes généraux du droit communautaire ».*
Mais il faudra attendre le Traité d'Amsterdam[1] pour voir s'étendre par son article 46 la compétence juridictionnelle de la Cour de Justice des Communautés Européennes à l'action des institutions. L'objectif étant de vérifier le respect des droits fondamentaux garantis à travers la référence que l'article 6 fait à la CEDH. C'est ainsi qu'a émergé un système commun de protection des droits fondamentaux. Le juge communautaire a systématisé les principes inscrits dans les Traités et a consacré des principes généraux du droit, comme les droits fondamentaux, dans l'ordre juridique communautaire.

Parmi les autres éléments à prendre en considération, concernant les droits de l'homme et l'Union européenne, il faut citer l'exigence du respect des droits fondamentaux en tant que condition préalable à l'adhésion de nouveaux états *«Tout Etat européen qui respecte les principes énoncés à l'article 6, paragraphe 1, peut demander à devenir membre de l'Union »* [2]. De plus, il existe des sanctions envers les Etats membres qui ne respectent pas ces principes. En fait, si le Conseil constate une violation grave et persistante des droits fondamentaux de la part de l'un des Etats membres, il peut, en statuant à l'unanimité sur proposition d'un tiers des Etats membres ou de la Commission, et après avis conforme du Parlement, décider de suspendre certains droits découlant des Traités communautaires, y compris le droit de vote au sein du Conseil.

La promotion des droits de l'homme a donc connu une évolution tout au long de la mise en place des Communautés Européennes. Les institutions communautaires y ont joué un grand rôle.

B. Les Droits de l'Homme et le Parlement européen :

Le Parlement européen s'est préoccupé de cette question dès les années 60, elle a fait l'objet de plusieurs débats, donné lieu à de nombreux rapports suivis du vote de résolutions. La commission avait envisagé, dès 1975, l'élaboration d'un catalogue de droits fondamentaux qui aurait répondu de façon plus spécifique aux besoins des Communautés, en couvrant des droits économiques et sociaux non visés par la Convention européenne. La Déclaration commune de l'assemblée du Conseil et de la Commission du 5 avril 1977[3], appuyée sur la jurisprudence de la Cour, a établi un engagement symbolique de ces institutions de respecter la CEDH.

---

1. signé le 02 octobre 1997
2. article 49 du Traité d'Amsterdam
3. JOCE C 103 du 24 avril 1977

L'Acte unique européen est resté vague sur la question des droits fondamentaux, malgré les propositions précises de certains états et du Parlement, dont la conférence de Luxembourg avait été saisie pour faire adopter un texte proclamant les droits fondamentaux. Les Etats signataires se sont déclarés *«décidés à promouvoir ensemble la démocratie en se fondant sur les droits fondamentaux reconnus dans les constitutions et lois des Etats membres et dans la CEDH ».* L'article 4 du projet du Parlement de 1984 de Traité de l'Union européenne comportait une formule beaucoup plus opérationnelle : *« l'Union protège la dignité de l'individu et reconnaît à toute personne relevant de sa juridiction les droits et libertés fondamentaux».* Faute de temps, le Parlement n'avait pas approfondi lors de l'adoption du projet la question de l'établissement d'un catalogue des droits de l'homme.

Le Parlement a ultérieurement repris ses travaux à la suite d'une proposition de résolution déposée par messieurs LUSTER et PFENNING relative au parachèvement du projet de Traité instituant l'Union européenne(1), la Commission institutionnelle a adopté en 1988 un livre blanc sur les libertés et droits fondamentaux(2) et le Parlement a organisé à Florence une audition publique sur les droits de l'homme dans l'Union(3). Il a adopté, le 12 avril 1989, une Déclaration des droits et libertés fondamentaux annexée à une résolution(4). Il a invité les autres institutions à s'associer à ce texte qui ne revêt aucune valeur contraignante, mais qui garantit un ensemble de droits civils et politiques.

Le Parlement est donc très sensible au problème des droits de l'homme. Il joue aussi un rôle moteur en obtenant à maintes reprises des résultats positifs suite à la dénonciation de violations. En effet, au cours de chaque session, une partie des travaux parlementaires est réservée à la dénonciation de cas de violation des droits de l'homme à travers le monde. Le Parlement a demandé et obtenu que, dans les relations entre l'Union et les pays tiers, l'accent soit placé sur le respect des droits de l'homme en tant que condition nécessaire pour bénéficier des avantages économiques escomptés.

Mais, il ne se borne pas à mettre en évidence et à condamner les violations aux droits fondamentaux, il adopte chaque année un rapport sur le respect de ces droits dans l'Union européenne(5). De plus, il s'est fixé l'objectif de financer des initiatives en faveur des droits de L'homme comme *l'initiative européenne pour la démocratie et la protection des droits de l'homme.*

Le Parlement européen ne manque donc pas de s'exprimer sur ses inquiétudes quant aux différentes négations des valeurs propres à l'Union, qui sont la dignité humaine, le respect et la coexistence pacifique. Le respect de la vie privée trouve donc sa place dans la protection que l'Europe offre aux droits fondamentaux.

---

1. PE 2-363/84
2. PE 115.274/déf.
3. PE 124.155
4. Résolution du 12 avril 1989, JOCE C120 du 16 mai 1989 p.51
5. Le dernier en date : par M. BARROS MOURA publié le 6 novembre 1998.

C. La place du respect de la vie privée dans la protection européenne des droits de l'homme :

Malgré les efforts des rédacteurs de la CEDH, cette dernière se présente souvent comme un texte encore lapidaire qui a dû être explicité et complété de manière très dynamique par la Commission et la Cour. Pour donner un exemple sur le sujet qui nous intéresse, la simple mention «respect de la vie privée et familiale» dans l'article 8 de la CEDH entraîne une quantité d'implications.

Le droit au respect de sa vie privée et familiale, du domicile et de la correspondance connaît donc une protection avec un champ d'application assez large. Interprétant la Convention comme un instrument «vivant » adapté aux conditions de la vie d'aujourd'hui, la Cour et la Commission ont analysé ces notions en considération de l'évolution des mœurs, des mentalités comme le progrès scientifique ou technique. Mais, ce large pouvoir d'interprétation n'est pas pour autant illimité.

L'extension du champ de protection de l'article 8 provient aussi du recours très fréquent en ce domaine aux obligations positives de l'état. Car la Convention consiste à protéger des droits concrets et effectifs c'est pourquoi elle appelle parfois à des mesures actives, positives de la part des états.

Ce développement montre bien l'importance croissante prise par les droits de l'homme dans tous les aspects de l'action communautaire. Passé sous silence dans les premiers actes de la Communauté, le respect des droits fondamentaux et en fait très vite devenu le fil directeur tant de l'intégration européenne que de l'affirmation de l'identité européenne. Le respect de la vie privée et donc le secret des correspondances font parti intégrante des droits de l'homme, ils connaissent donc une protection en Europe notamment contre la surveillance électronique qui est réglementée.

2) Surveillance électronique et réglementation :

Les techniques de surveillance peuvent être définies comme des dispositifs ou des systèmes capables de surveiller, de suivre et d'évaluer les mouvements des personnes, des biens ou autres avoirs. Dans les années quatre-vingts, de nouvelles formes de surveillance électroniques sont apparues ce qui a consisté à automatiser l'interception de communication. Pour bien cerner le problème, étudions premièrement les interceptions légales pour ensuite envisager plus précisément les interceptions globales de communication et leur risque.

A. Les interceptions légales :

Le respect du secret des correspondances doit faire l'objet de conciliation avec d'autres principes tout aussi important comme l'ordre public et la sécurité nationale. Donc certaines atteintes sont permises à l'encontre de ces droits mais seulement dans certains but et si celles-ci sont légales.

1. Réglementation communautaire et la position du Parlement européen :

Les interceptions légales de communications portent atteinte au respect de la vie privée et peuvent entraîner un stockage de données qui auront été interceptées.

Il semble donc judicieux, d'examiner la réglementation concernant la protection des données à caractère personnel dans le secteur des télécommunications, car celle-ci englobe une partie de l'activité mis en cause c'est à dire la surveillance électronique. Pour ensuite, étudier plus précisément la législation en vigueur sur les interceptions légales de télécommunication.

- La protection des données à caractère personnel dans le domaine des télécommunications :

La Convention citée dans l'introduction, qui a été signée le 28 janvier 1981, a trait à la protection des personnes à l'égard du traitement des données, elle énonce des principes protecteurs de la vie privée, mais ce ne sont que des principes généraux non contraignants c'est pourquoi le droit dérivé a été utilisé.

Le 25 octobre 1995, le Parlement européen et le conseil ont arrêté la directive 95/46/CE[1] relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de celles-ci. Elle a été adoptée après une proposition de la commission[2], concernant l'harmonisation des dispositions nécessaires pour assurer un niveau équivalent de protection de la vie privée, dans les Etats membres, ainsi que la libre circulation des équipements et services de télécommunications dans la communauté, et suite à l'avis du comité économique et social du 03 avril 1991[3].

La directive rappelle que «les systèmes de traitement des données sont au service de l'homme ; qu'ils doivent respecter les libertés et droits fondamentaux des personnes(…) », c'est pourquoi dans son article premier, elle invite les Etats membres à assurer «la protection des droits et libertés fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données ». L'article 29 de la directive a institué le groupe de protection des personnes à l'égard du traitement des données à caractère personnel. Ce groupe est tenu de communiquer à la Commission, au Parlement européen et au Conseil un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté et dans les pays tiers.

Un premier rapport a été adopté le 25 juin 1997 par le groupe de protection des personnes, il couvre les principaux faits nouveaux observés en 1996 dans ce domaine. Puis, un deuxième rapport a vu le jour le 30 novembre 1998 qui reprend pour l'essentiel la structure du premier, et met en avant les évolutions enregistrées en la matière dans l'Union européenne.

Le processus de mise en œuvre de la directive a été enclenché en 1996 dans tous les états et au niveau européen. Les institutions européennes et la Commission en particulier traitent couramment des données personnelles dans le cadre de leurs activités. Au moment de son adoption, la Commission et le Conseil se sont engagés, dans une déclaration publique[4], à respecter la directive et ont invité les autres institutions et organes communautaires à en faire de même.

---

1. JO L 281 du 23.11.1995 p.31
2. Présenté le 14 juin 1994 JO C 200 du 22/07/1994 p.4
3. JO C 159 du 17/06/1991 p. 38
4. Cette déclaration a été publiée le 24 juillet 1995 9012/95 (Presse226)

Bien que la directive constitue l'élément clé de la politique européenne en matière de protection des données, elle est complétée par un certain nombre d'autres initiatives qui visent à garantir au citoyen un cadre de protection cohérent.

Le Parlement européen et le conseil ont arrêté, le 15 décembre 1997, la directive[1] concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (elle a été prise suite à la position commune adoptée par le Conseil des ministres le 12 septembre 1996 qui a été suivi d'une procédure de conciliation).

Cette directive a pour objet de garantir la libre circulation dans la Communauté des données et des équipements et services de télécommunication en harmonisant le niveau de protection des abonnés et des utilisateurs des services publics de télécommunications à l'égard du traitement des données à caractère personnel dans le secteur des télécommunications. La directive précise, pour le secteur des télécommunications, les règles générales énoncées dans la directive 95/46/CE et elle renforce la protection de la vie privée et des intérêts légitimes des abonnés.

Donc cette directive est étroitement liée à la directive générale sur la protection des données (adoptée le 24 octobre 1995), car elle précise, pour le secteur des télécommunications, les règles générales déjà posées par l'autre directive. Mais son champ d'application est plus étendu, elle couvre les droits et intérêts légitimes des personnes et englobe des aspects de la vie privée qui ne sont pas directement liés au traitement des données. La directive contient des dispositions sur : - la sécurité des informations transmises sur les réseaux publics de télécommunications ; - la confidentialité des communications ; les limites de l'étendue et de la durée du traitement des données relatives au tarif ; - l'identification des appels malveillants ; - la protection de la vie privée eu égard aux appels non sollicités.

Remarque : 1- Le Conseil de l'Europe a poursuivi les travaux qu'il mène régulièrement sur les questions de protection des données. Le Comité des ministres a adopté deux recommandations : - celle adoptée le 13 février 1997 n° R(97)5 ; - et celle adoptée le 30 septembre 1997 n° R(97)18.

2- Le groupe de protection des personnes, à la suite de discussions, a adopté un certain nombre de documents, comme la recommandation 1/97 sur la protection des données et les médias[2], l'avis 1/97 sur l'initiative canadienne concernant la normalisation en matière de protection de la vie privée[3], la recommandation 3/97 concernant l'anonymat sur Internet[4].

La protection des données à caractère personnel connaît donc une réglementation précise avec les deux directives citées ci-dessus, mais faut ajouter aussi que le traité d'Amsterdam a trait à ce problème en incluant une disposition spécifique sur la protection des données personnelles.

---

1. Directive 97/66/CE JO L 24 du 30/01/1998
2. Document WP1 – 5012/97
3. WP2 – 5023/57
4. WP6 – 5057/97

Il est évident que la directive qui nous intéresse le plus et celle qui a été adopté le 15 décembre 1997 (97/66/CE), car elle concerne «le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications » et traite particulièrement du problème de la confidentialité des communications dans son article 5 : *« Les états membres garantissent au moyen de réglementations nationales, la confidentialité des communications (...). En particulier ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter de stocker les communications ou de soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées. »*

Le droit au respect de la vie privée peut donc, selon cette directive, être atteint par des interceptions légales de communications. Il nous faut donc étudier la réglementation s'y rapportant.

- Les interceptions légales de télécommunications :

Les dispositions européennes concernant les interceptions légales sont moins contraignantes et abondantes que celles réglementant le stockage de données à caractère personnel. En effet, dans ce domaine, les institutions européennes ne se sont servies jusqu'à présent que de résolutions. C'est-à-dire des actes qui ne comportent aucune procédure d'engagement juridique et qui traduisent seulement une volonté politique des états, qui leur confèrent donc seulement valeur d'orientation pour guider et programmer leurs actions. De plus, les résolutions en la matière sont loin d'être abondantes. Une seule a été prise par le Conseil, le 17 janvier 1995, et il a fallu attendre 1998 pour qu'un nouveau projet soit adopté.
Il est important de noter que cette réglementation doit suivre les progrès réalisés dans le domaine de la surveillance électronique, car aujourd'hui, par exemple, l'utilisation de microphones miniatures pour intercepter les télécommunications est une technologie dépassée. En effet, les *espions modernes* peuvent acheter des ordinateurs portables adaptés à cet effet et se régler tout simplement sur tous les téléphones mobiles branchés dans le secteur en déplaçant le curseur sur le numéro de ces appareils.

La question est, semble-t-il, de savoir si la position du Conseil, en adoptant ces résolutions, permet un réel respect de la vie privée. La résolution adoptée le 17 janvier 1995[(1)]doit être transposée dans son contexte pour bien la comprendre.

Dans l'Union européenne, les personnes privées ne peuvent et ne doivent pas être sujettes d'interceptions illégales concernant leur vie privée, grâce aux accords internationaux et à la CEDH. Mais la plus part des états ont une réglementation propre concernant les interceptions légales. Les Etats-Unis ont eux une protection limitée de la confidentialité, car les intérêts qui peuvent en ressortir sont énormes notamment dans le domaine économique. C'est ainsi que ces derniers sont derrière un effort international allant dans le sens d'une augmentation des capacités d'interception. Ils ont adopté une loi : CALEA, en 1994, qui oblige les fabriquants de télécommunications à faciliter les interceptions de communication. Mais, ne s'arrêtant pas là, ils souhaitaient que les Etats membres de l'Union incorporent CALEA dans les lois européennes.

---

1. Résolution du Conseil du 17 janvier 1995 : JO C 329 du 04/11/1996 p.1 à 6

C'est ainsi, que le Conseil des Ministres a adopté la résolution de janvier 1995 sous l'influence des Etats-Unis, car cette dernière reprend les souhaits invoqués par la première puissance mondiale. Cette résolution n'a été publiée que deux ans après son adoption, et le Conseil n'a pas demandé l'avis du Parlement. Elle permet, à ce dernier, d'énumérer une série de spécifications qui doivent être prises en compte par les Etats membres lors d'interceptions légales des télécommunications. Elles doivent garantir un niveau technique commun lors de l'exécution d'interception, ainsi les capacités d'intercepter seront plus grandes. Il est impératif de disposer de normes comparables, d'une part en raison de l'importance des interceptions dans le cadre de lutte contre la criminalité organisée au niveau international, et, d'autre part, parce que ces normes simplifient les interceptions effectuées en réponse à des commissions rogatoires. Il est tout aussi impératif, et cela est évident, que les interceptions soient exécutées dans ces seuls buts. Ainsi, une réelle conciliation entre le respect de la vie privée et la sécurité publique sera possible.

Le progrès technique a permis de mettre sur le marché des nouvelles technologies de télécommunications. Il paraît donc nécessaire de mettre «au goût du jour» la résolution de 1995.

C'est donc, en partant du constat que les nouvelles technologies sont en permanente évolution, que le Conseil a adopté un projet de résolution, le 03 décembre 1998, qui propose de prendre une série de mesures en vue d'étendre les dispositions de sa résolution de janvier 1995. Ce projet de résolution présente par conséquent une annexe explicative proposant les modifications applicables aux communications utilisant les nouvelles technologies. Il vise donc à modifier la première résolution pour l'adapter à l'évolution technologique. Par lettre du 27 janvier 1999, le Conseil a consulté le Parlement (conformément à l'article K6 du traité CE), sur ce projet. Au cours de la séance du 12 avril 1999, le Président du Parlement a annoncé qu'il avait renvoyé ce projet, pour examen, à la commission des libertés publiques et des affaires intérieures et, pour avis, à la commission juridique et des droits des citoyens, ainsi qu'à la commission économique, monétaire et de la politique industrielle.

La commission des libertés publiques et des affaires intérieures a rendu son rapport[1] le 23 avril 1999. Celui-ci contient l'avis[2], de la commission juridique des droits des citoyens, adopté le 25 mars 1999, rejette la proposition du conseil qui selon elle est trop imparfaite et imprécise et donc cela pourrait porter préjudice aux droits des individus. Le rapport, quant à lui approuve la proposition avec quelques modifications et propose que le Parlement soit à nouveau consulté au cas où le Conseil apporterait des modifications substantielles à celles du présent rapport. Ainsi en adoptant le rapport, le 07 mai 1999, par le vote d'une résolution législative, le Parlement approuve le projet de résolution du Conseil, mais rappelle l'impérieuse nécessité de respecter la protection des données à caractère personnel. Il demande donc au Conseil de vérifier avant le 01 juillet 2000 dans quelle mesure les Etats membres ont transposé cette résolution ainsi que celle de 1995.

Rappelons que la résolution de 1995, pas plus que celle dont le projet a été adopté en 1998, n'a un caractère juridiquement contraignant pour les Etats membres. Il n'y a donc pas de réglementation européenne des écoutes téléphoniques et plus généralement, de l'interception légale de télécommunications. Au niveau national, les procédures prévoient, que ces écoutes téléphoniques se font par la police sur la base d'une autorisation du ministre compétent ou d'une commission rogatoire délivrée par un magistrat.

---

1. Rapporteur : G. SCHMID PE 229.986/déf .
2. Rapporteur pour avis : LUIGI A. FLORIO 99/0906(CNS)

Une présentation succincte ainsi faite de la législation en vigueur dans la Communauté sur la protection des données à caractère personnel et sur les interceptions légales, étudions maintenant son application dans les Etats membres.

2. L'application dans les états membres :

- Application de la réglementation concernant la protection des données :

Des progrès ont été accomplis au cours de l'année 1997 concernant la transposition des directives en droit national des Etats membres. Nous allons dresser un inventaire de la situation de chaque état.

BELGIQUE :Une loi du 11 décembre 1998 transposant la directive 95/46/CE du Parlement européen et du Conseil a été adoptée.

DANEMARK : Une loi de juin 1998 va dans le même sens que celle de Belgique.

GRECE : la loi grecque sur la protection des données a été ratifiée par le parlement hellénique le 26 mars 1997, publié le 10 avril 1997.

ESPAGNE : Un projet de loi a été discuté par le parlement dans le courant de l'été 1998. Mais la plupart des dispositions ont cependant déjà été transposées par la « Ley Organica » du 29 octobre 1992.

ITALIE : La loi sur la protection des données à caractère personnel a été adoptée le 31 décembre 1996. Le parlement a autorisé le gouvernement à légiférer par voie réglementaire pour la modifier et la compléter en vue de la transposition de la directive, ce qui a été fait le 06 octobre 1998.

AUTRICHE : La révision du projet de transposition de la directive a été adoptée par le parlement le 18 octobre 1998.

PORTUGAL : la constitution a été révisée par une loi constitutionnelle du 20 septembre 1997 afin de pouvoir transposer la directive. Un projet de loi fût présenté au parlement le 02 avril 1998 et adopté le 26 octobre 1998.

SUEDE : La nouvelle législation sur la protection des données a été adoptée par le parlement le 16 avril 1998 et des mesures complémentaires réglementaires en septembre 1998.

ROYAUME-UNI : Adoption d'une loi en juillet 1998 sur la protection des données transposant la directive.

Les autres Etats de l'Union n'ont pas encore des références concernant cette réglementation, c'est à dire qu'ils n'ont pas encore adopté de loi régissant la protection des données à caractère personnel. Par exemple, la France a seulement mis en œuvre un rapport adressé au Premier ministre en mars 1998, et l'autorité française responsable de la protection des données, la *commission nationale de l'informatique et des libertés,* sera consultée au sujet des avant-projets de loi. Ou, pour donner un autre exemple, la Finlande n'a pas encore de législation en la matière puisque les mesures nécessaires pour appliquer la directive, qui incluront des modifications de la loi de 1988 sur la protection des données, sont en cours d'élaboration.

En ce qui concerne la directive du 15 décembre1997, les Etats membres avaient jusqu'au 24 octobre 1998 pour la transposer, sauf pour ce qui se rapporte à certains aspects de la confidentialité des communications, pour lesquels un délai supplémentaire a été convenu, soit jusqu'au 24 octobre 2000.

- La position des Etats membres concernant les interceptions légales de communications :

Comme nous l'avons dit, il n'existe pas de réglementation européenne contraignante qui a trait aux interceptions légales, chaque état a donc sa propre législation en la matière, mais il est vrai que les réglementations des Etats membres sont quelque peu similaires.

Il n'y a donc pas de contrôle opéré par la Cour de justice des Communautés Européenne car aucun problème de transposition ne peut être invoqué, pourtant ces réglementations ne sont pas exemptes de toutes vérifications. En effet, tout Etat membre doit avoir ratifié la CEDH, donc les législations concernant les interceptions légales vont être contrôlées par rapport à cette convention, par l'organe juridictionnel institué : la Cour Européenne des Droits de l'Homme.

Les réglementations nationales devront donc être adéquates avec la convention et par conséquent ne pas aller à l'encontre des principes énoncés, comme le respect de la vie privée, familiale et du secret des correspondances (article 8), sous peine d'une condamnation de la Cour.

La jurisprudence de celle-ci a montré que les droits fondamentaux n'ont pas toujours été respectés dans la mise en œuvre d'interceptions légales de télécommunications. Par exemple, le Royaume-Uni a été condamné, le 2 août 1984, dans l'arrêt MALONE, car il a eu violation de l'article 8 de la CEDH par des interceptions (judiciaires) de communications. En effet, la Cour rappelle que l'existence d'une législation autorisant à intercepter des communications pour aider la police judiciaire à s'acquitter de ses tâches peut-être nécessaire « à la défense de l'ordre et à la prévention des infractions pénales ». Cependant, le système de surveillance adopté doit s'entourer de garanties suffisantes contre les excès, ce qui n'était pas le cas pour la réglementation anglaise.

Le contrôle et donc nécessaire est efficace, car comme nous allons le voir les différents pays incriminés ont, après une condamnation, adaptés leur législation au respect des droits de l'homme et plus précisément au respect du secret des correspondances. Pour illustrer cette affirmation, prenons l'exemple de la France qui a été condamnée par la Cour Européenne des Droits de l'Homme, et a ensuite aligné sa législation à la CEDH.

En matière d'écoute téléphonique, la jurisprudence de la Cour a eu des répercussions importantes et directes en droit interne français. Dans deux arrêts prononcés le 24 avril 1990 dans les affaires KRUSLIN et HUVIG, la Cour Européenne des Droits de l'Homme a, pour l'essentiel, confirmé les solutions retenues pour l'arrêt MALONE. La Cour a estimé que les garanties données au justiciable soumis à des écoutes téléphoniques ordonnées par le juge d'instruction étaient imprécises ou insuffisantes. Eu égard à la gravité de l'atteinte à la vie privée qui résulte d'une écoute téléphonique faite à l'insu des usagers du téléphone, il est nécessaire que le législateur élabore des règles détaillées et précises sur ce point. La Cour a donc conclu à la violation de l'article 8. Une certaine qualité de la loi est donc exigée, c'est ainsi que le législateur français a élaboré une nouvelle loi, du 10 juillet 1991, qui réglemente les interceptions de communications en s'efforçant d'équilibrer le maintien de la sûreté de l'état et le respect du secret des correspondances téléphoniques.

Nous avons exposé ici les arrêts de principe de la Cour de Strasbourg, la jurisprudence étant abondante une liste exhaustive serait impossible ici. Il est vrai que des arrêts récents existent sur ce sujet et de nouvelles affaires vont certainement voir le jour, en tenant compte des nouvelles technologies apparues dans le domaine des interceptions. Les législations vont donc devoir s'adapter et introduire ces nouveaux moyens d'écoute. Tout un arsenal de dispositif d'écoute a été développé pour enregistrer les communications et intercepter les télécommunications. Les écoutes de communication judiciaires et administratives, celles dont la réglementation a été vue ci-dessus, font piètre figure face aux réseaux d'interceptions gouvernementaux opérant à l'échelon national et international.

B. Les interceptions globales :

Pour bien comprendre ce que le terme « interception globale » signifie, nous allons tout d'abord en faire une description succincte, pour ensuite examiner les risques qu'elles peuvent engendrer puis les réglementations existantes à ce sujet. Toutes les informations relatées ici sont tirées des différentes études présentées en première partie ainsi que de l'étude "Une évaluation des techniques de contrôle politique"[(1)] de la STOA.

1. Description :

Les systèmes de surveillance globale facilitent la surveillance de masse de toutes les télécommunications, y compris le téléphone, les transmissions par FAX et par courrier électronique, qu'il s'agisse de celles des citoyens privés, des hommes politiques, des syndicalistes ou des entreprises privées.

Les interceptions globales sont possibles grâce à la *COMINT*, la recherche de communications électroniques qui est une activité industrielle permettant d'intercepter toutes les communications étrangères, utilisée essentiellement à des fins militaires, elle s'est développée au cours de la Guerre Froide où l'espionnage était de rigueur. La plupart des pays développés utilisent la *COMINT,* soit de façon isolée, soit en partenariat avec d'autres nations. L'organisation la plus importante est sans nul doute celles des nations anglophones : *UKUSA*. Ces nations opèrent avec un système dénommé *ECHELON*. Ce système vise, aujourd'hui, essentiellement des cibles non militaires. Il fonctionne en interceptant sans distinction un très grand nombre d'informations puis en triant les éléments intéressants à l'aide d'un système d'intelligence artificielle. Cinq nations se partagent les résultats, les Etats-Unis étant partenaire principal en vertu de l'accord *UKUSA*, La Grande-Bretagne, le Canada, la Nouvelle Zélande et l'Australie qui ont un rôle subalterne de fournisseur d'informations.

La NSA, National Security agency, est l'organisme qui utilise *ECHELON* aux Etats-Unis. Elle est chargée du contre espionnage, de la protection des communications gouvernementales et militaires, elle se consacre aussi à la recherche et au développement. Elle couvre tout le champ des technologies de l'information militaire et civile.

Le pacte *UKUSA* date de 1947, ses attributs sont montés en puissance dans les années 70 et 80 quand fût mis en place le réseau *ECHELON*. On peut se demander qu'elle est la place de L'Union européenne dans ces systèmes. Les Etats membres, qui semblent s'inquiéter de la prédominance des nations anglophones c'est-à-dire celles appartenant au pacte UKUSA, ne sont pas sans reste. En effet, ces derniers semblent suivre la position de l'Union, qui met en œuvre un projet de surveillance électronique analogue à *ECHELON*.

---

1. PE166.499/int.St./Exect.Sum./fr. 14 septembre 1998

C'est en prônant la lutte contre la criminalité que les politiques, la police, les douanes cherchent à étendre leur capacité de surveillance. Ces travaux sont menés sous l'égide du conseil des ministres de l'Union européenne et se distinguent par leur opacité.

M. Glyn Ford, membre britannique du Comité des libertés civiles et des affaires intérieures du Parlement européen, rappelle que « quelques exigences élémentaires devraient être respectées. Il faut qu'il y ait une certaine maîtrise de ce qui est surveillé et une dose de contrôle parlementaire, européen et national. Nous n'avons pas d'objection de principe au fait qu'il y ait des écoutes, mais la lutte contre le terrorisme et les filières de blanchiment ne peut servir de prétexte à l'écoute d'Amnesty internationale ou à l'espionnage économique. »[1]

Il faut rajouter, qu'avec les modifications techniques des réseaux de télécommunication un flou inquiétant est laissé en ce qui concerne les modes de contrôle de ces écoutes et la protection juridique qui permettrait de sauvegarder ce droit fondamental qu'est le respect de la vie privée.

Les interceptions globales qui permettent d'obtenir des informations sur des organisations terroristes ou criminelles ne posent en vérité pas de problème, mais là où des questions peuvent se poser, c'est lorsque des informations recueillies sont utilisées à des fins différentes, comme économiques par exemple.

2. Les risques possibles :

Personne ne nie le rôle de ces réseaux dans les opérations de lutte contre le terrorisme, le narcotrafic, le blanchiment de l'argent et le commerce illicite des armes, mais l'ampleur du réseau d'interception des communications étrangères suscite bien des craintes quant à la législation, sur les systèmes de protection des données et de la vie privée en vigueur dans les Etats membres. Cette dernière est supposée protéger la confidentialité entre les citoyens et les entreprises de l'Union et des pays tiers. De plus, des risques économiques, c'est-à-dire l'abus d'information à des fins commerciales, peuvent être engendrés par ce type d'interception.

Certains journalistes n'ont pas hésité à affirmer qu'*ECHELON* avait été utilisé pour avantager des entreprises américaines impliquées dans des contrats d'armement, pour renforcer la position de Washington dans d'importantes négociations relatives à l'organisation mondiale du commerce avec L'Europe lors des différents avec le Japon sur les exportations des pièces détachées automobiles. Si ces exemples s'avèrent exacts les risques engendrés peuvent être importants, comme la perte de beaucoup de contrats par les entreprises de l'Union européenne.

Une[2] des études, que nous avons présenté en première partie, donne quelques exemples d'utilisation abusive d'informations économiques intercepter par des réseaux globaux comme *ECHELON*. Nous pouvons citer le contrat, qui est passé « sous le nez » de la France, en janvier 1994. Il s'agissait d'un contrat de 30 millions de francs avec l'Arabie Saoudite pour la vente d'armes qui s'est retrouvé entre les mains d'une compagnie américaine : McDonnell-Douglas, rival d'Airbus, car celle-ci avait eut connaissance, grâce au système électronique d'écoutes, des conditions financières données par Airbus.

---

1. Le monde diplomatique mars 1999
2. The draft final study juin 1999

Le Sunday Times[1] a, quant à lui, relaté que les Français se sont plaints, que Thomson, l'entreprise électronique française, avait perdu un contrat de 1,4 millions de dollars destiné à la fourniture d'un système radar au Brésil parce que les Américains avaient intercepté des détails des négociations et les avaient transmis à la compagnie américaine Raytheon qui avait par la suite remporté le contrat.

Face à un tel système les Européens peuvent être tétanisés. Mais en l'absence de preuves de l'utilisation d'*ECHELON* pour l'espionnage économique, on hésite à compromettre les « bonnes relations économiques avec les Américains ». [2]

3. La position de l'Union européenne et du Parlement sur les réseaux globaux d'interceptions (et donc les relations transatlantiques) :

« Alors que l'Europe fait mine de s'inquiéter de l'espionnage électronique mené dans le monde entier par les Américains, ses polices préparent à leur tour, dans la plus grande discrétion, un projet de surveillance du téléphone et d'Internet. »[3]

En janvier 1997, Statewach, une organisation de surveillance et de recherche sur les libertés publiques basée au Royaume-Uni, indiquait que l'Union européenne avait secrètement accepté la création d'un réseau international d'écoutes téléphoniques via un réseau secret de commissions créées dans le cadre du troisième pilier du Traité de Maastricht couvrant la coopération dans les domaines juridiques et le maintien de l'ordre. Les principaux points de ce plan sont soulignés dans un protocole d'accord, signé par les Etats de l'Union en 1995[4], sans aucune réunion préalable du conseil.

Suite à ces informations, qui par ailleurs ont été mises en avant par l'étude de la STOA « une évaluation des techniques de contrôle politique »[5], une discussion a été ouverte au Parlement. C'est ainsi, que plusieurs parlementaires ont questionné la Commission et le Conseil à propos d'*ECHELON* et des systèmes globaux de surveillance.

Ces questions ont entraîné le vote d'une résolution. Elles s'appuient sur les différents documents que nous vous avons déjà cités, comme les diverses études de la STOA. La Commission donne une image assez étrange quant à sa position sur le sujet, car elle condamne ouvertement toutes atteintes à la vie privée notamment par le biais d'interceptions de communications, mais d'un autre côté elle se déclare incompétente pour engager une initiative qui permettrait d'éviter que les Etats membres s'espionnent mutuellement[6]. De plus concernant la question[7] de prendre des mesures contre les pays appartenant à l'alliance UKUSA, la Commission reste muette. Elle rappelle simplement qu'elle « condamne toute tentative de violation de l'intégrité et de la confidentialité des informations détenues ou transmises par les institutions. »

---

1. Le 11 mai 1998
2. Le monde diplomatique mars 1999 : « Grandes oreilles » américaines par Philippe Rivière
3. Le monde diplomatique mars 1999 : Tous les Européens sur écoutes par Philippe Rivière
4. ENFOPOL 112 10037/95, 25.10.95
5. Septembre 1998 PE 166.499
6. Question écrite à la Commission E- 1040/98 du 06 avril 1998
7. Question écrite à la Commission E- 1306/98 du 29 avril 1998

Mais il faut tout de même ajouter, que la Commission préconise une libéralisation du chiffrement pour protéger la confidentialité des communications (voir partie ci-dessous). Quant au Conseil, une question lui a été adressée le 08 juin 1998[1] concernant le système de surveillance *ECHELON*, à laquelle il n'a pas répondu, donc sa position reste assez floue. Mais nous savons tout de même que ce dernier a décidé d'introduire un système de surveillance analogue dans le troisième pilier.

Le Parlement a donc adopté une résolution[2], après plusieurs propositions de parlementaires, le 16 septembre 1998, sur *ECHELON* et les relations transatlantiques. Dans cette dernière, il reconnaît la nécessité des systèmes de surveillance électronique mais insiste sur le fait qu'il est essentiel que l'on puisse s'appuyer sur des systèmes de contrôle démocratique et il demande ainsi qu'une plus grande protection soit mise en place, en adoptant un code de conduite par exemple et en discutant de ces problèmes au niveau des parlements nationaux et communautaire. De plus, il insiste sur l'importance des relations entre les Etats-Unis et l'Union européenne mais il suggère une plus grande transparence, une implication plus importante du Parlement européen dans ces dernières, car l'ensemble des décisions ayant trait à ceci sont prises par la Commission et le Conseil. (Le texte intégral de cette résolution est inséré en annexe.)

Les interceptions de communication, la surveillance électronique engendrent donc comme nous venons de le voir des atteintes aux droits fondamentaux notamment le respect de la vie privée. Mais, il existe aujourd'hui des techniques qui permettent de préserver la confidentialité : le cryptage, le chiffrement, mais celles-ci rencontrent certains obstacles dans leur utilisation.

3) Cryptographie et chiffrement : la clef du problème ?

A. Présentation et problématique :

« Bien qu'il soit difficile de quantifier les pertes causées par l'espionnage industriel, il est raisonnable d'estimer à plusieurs milliards d'euros par an les déperditions financières au niveau des entreprises de la Communauté Européenne. »[3]

Le chiffrement est un moyen de lutter contre ce type d'espionnage, puisque s'est un processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible. Il existe deux types de cryptographie : - la cryptographie symétrique et – celle asymétrique. La cryptographie est donc l'étude de techniques permettant d'assurer la confidentialité. Dans le contexte d'une société où les échanges d'informations numériques se développent, il est indispensable de pouvoir bénéficier de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel, assurer la transaction financière ou commerciale, passer des contrats en l'absence de support papier. Les technologies cryptographiques sont de nos jours reconnues comme étant des outils essentiels de la sécurité et de la confiance dans les communications électroniques.

---

1. Question écrite E- 1775/98
2. Résolution B4-0803/98 16/09/98 JOCE 12/10/1998 C313 p.98
3. « ENCRYPTON AND CRYPTOSYSTEM IN ELECTRINIC SURVEILLANCE » STOA PE 168/184/part3/4

Mais, si l'on crypte les messages et les fichiers avec des moyens puissants, le contenu des informations devient indéchiffrable pour tous, y compris pour l'état. Or l'état et la justice veulent pouvoir intercepter les communications échangées et accéder au contenu des fichiers dans les cas prévus par la loi, dans le cadre de la lutte contre la délinquance, le crime et pour assurer la sûreté de l'état. De plus, la sécurité des transmissions électroniques ne peut être garantie que par une cryptographie forte, et le développement du commerce électronique qui par sa nature est international, suppose la possibilité de pouvoir importer et exporter librement des données cryptées. Cependant, ces besoins se heurtent à diverses restrictions à la libre exportation des produits de chiffrement. En effet, les produits de cryptographie font partis des biens considérés comme « sensibles » ou « à double usage » (c'est à dire utilisés civilement ou militairement).

C'est ainsi, pour ces diverses raisons, que le chiffrement connaît une réglementation stricte qui varie selon les différents états. L'Union européenne a une position intéressante sur la question mais elle n'est pas suivie par tous les états membres.

B. La position de l'Union européenne :

Un règlement communautaire du 19 décembre 1994[(1)] institue un régime de contrôle des exportations de biens à double usage afin d'établir des normes communes dans le cadre de la réalisation du marché commun. Conformément à l'article 19 du règlement, les Etats membres doivent mettre en œuvre une procédure d'octroi de licence pour une période transitoire en ce qui concerne le commerce intra-communautaire de certains produits sensibles, par exception au principe de libre circulation, pour le moment cela concerne aussi les produits de chiffrement. Cela signifie que le règlement oblige les Etats membres à imposer non seulement des contrôles à l'exportation sur les produits à double usage, mais aussi des contrôles intra-communautaires sur les produits cryptographiques expédiés d'un Etat membre vers un autre.

Mais, l'objectif premier de ce texte est de créer une procédure de contrôle harmonisée pour les exportations hors de l'Union. Les produits concernés sont cités en annexe du texte, en ce qui concerne la cryptographie sont ainsi visés les télécommunications, logiciels et matériels informatiques de haute technologie et la sécurité de l'information. Toutefois, les logiciels qui sont couramment à la disposition du public ne sont pas soumis à ces contrôles.
Actuellement, ce règlement est en cours de révision par les institutions communautaires. En effet, la période transitoire devait prendre fin le 1er juillet 1998 : à compter de cette date, les exportations des produits de chiffrement à destination de l'Union européenne auraient du être libre. Il faut noter qu'un accord international fut signé deux ans plus tard reprenant les mêmes objectifs : l'accord de WASSENAAR. Il a été adopté le 11 et 12 juillet 1996 par trente-trois pays parmi la plupart des pays européens, il remplace l'accord COCOM. Il contrôle à l'exportation des procédés de cryptographie en tant que biens à double usage, cependant il préconise l'exemption de ces contrôles pour les logiciels grand publics.

Mais, la réglementation communautaire ne s'est pas arrêtée là, en effet on peut noter que certaines initiatives ont encore été prises par les institutions. La Commission a présenté le 15 mai 1998, un rapport dressant le bilan de l'application du règlement vu ci-dessus, et une proposition de règlement[(2)] visant à remédier aux lacunes recensées dans le règlement précité.

---

1. Règlement, 3381/94 du Conseil
2. COM(98)257final JOCE 15-05-98 L257

Le régime mis en place en 1994 a permis de réduire les formalités d'exportation et de faciliter la libre circulation de la quasi-totalité des biens à double usage dans la Communauté. Cependant, le régime présente des lacunes concernant le mécanisme commun de contrôle à l'exportation. En effet, il existe un manque de cohérence entre les différentes politiques et pratiques nationales.(voir le cas de la France dans la partie ci-dessous)
Les Etats restent en fait en désaccord sur les politiques d'exportations prises sur la base d'autorisation.

La proposition de règlement tente de résoudre ces problèmes afin de faciliter et de simplifier les exportations de bien à double usage. Cette simplification est illustrée par la mise en place de formulaires nationaux uniformisés concernant les autorisations à l'exportation. Les Etats membres ont toujours la faculté d'accorder une licence d'exportation à un produit alors qu'un autre l'a refusé, mais une obligation de motivation et des consultations préalables sont imposées, de la part de l'état qui décide d'autoriser l'exportation. La Commission assouplit le régime et concilie la volonté des états en les informant et en leur donnant la possibilité de surveiller et de contrôler les exportations. La proposition supprime concernant les produits de cryptologie les restrictions existantes aux transferts intra-communautaire et les remplace par une procédure de notification.

Rappelons que cette proposition de règlement s'inscrit dans un cadre d'ensemble d'une politique communautaire. En effet, l'Union s'est fixée comme objectif de parvenir d'ici l'an 2000 au développement d'une politique de libres circulations des produits et service de cryptographie. On peut citer notamment dans le cadre de cette politique, la proposition de directive concernant la signature électronique[1] qui permet de bien distinguer la cryptographie utilisée pour l'authentification, et celle utilisée pour garantir la confidentialité des données. Cette proposition a été approuvée par le Parlement européen, sous réserve des modifications qu'il y a apporté, par la résolution législative du 13 janvier 1999[2] qui fait suite à un rapport de la commission juridique et des droits des citoyens[3] du 16 décembre 1998. Comme le Parlement a émis des modifications, une proposition modifiée de directive du Parlement et du Conseil[4] sur un cadre commun pour les signatures électroniques, présentée par la Commission comme le prévoit le traité CE, a été adoptée le 29 avril 1999.

Nous remarquons ici, que le Parlement intervient dans la mise en œuvre de la réglementation communautaire. Cependant, il devrait intervenir encore plus souvent et prendre position en faveur d'une libéralisation de l'usage de la cryptographie sur l'ensemble du territoire communautaire, c'est ce qu'avance les études élaborées par la STOA que nous avons présenté ci-avant.

La cryptographie par les implications qu'elle a en matière de vie privée et de protection des données, soulève des questions mettant en jeu des choix de société. La réglementation européenne n'étant pas encore harmonisée, elle diffère quelque fois des législations nationales comme c'est le cas de la France.

---

1. prise le 13 mai 1998 COM(98)297
2. COM(98)297 JOCE C104 14/04/1999 p.49
3. PE 228.030/déf.
4. COM/99/0195

C. Position divergente d'Etat membre : le cas de la FRANCE :

Dans un contexte où les échanges d'information électronique se développent, il est indispensable de pouvoir bénéficier de systèmes sécurisés pour protéger les données, assurer la sécurité des transactions financières et commerciales. Le chiffrement est très souvent le seul moyen efficace pour répondre à ces exigences. Les technologies cryptographiques sont ainsi reconnues comme étant des outils essentiels de la sécurité et de la confiance dans les communications électroniques. Les besoins de confidentialité de l'utilisateur ont été mis en avant par la loi du 26 juillet 1996[1], qui fait référence à la protection des informations et au développement des communications et des transactions sécurisées. Cependant, la France, invoquant la nécessité de préserver les intérêts de la défense nationale a maintenu une réglementation contraignante de la cryptographie. En effet, plus d'un an et demi après la loi de 1996, des décrets ont été publiés, ces derniers ne mettent pas en œuvre la libéralisation annoncée, mais illustre une logique sécuritaire ancrée.

La législation française distingue d'une part les fonctions d'authentification et d'intégrité des données, soumises à un régime plus libéral, et les fonctions de confidentialité, sur lesquelles l'Etat entend garder un contrôle étroit. Mais, pour permettre aux utilisateurs de bénéficier de technique de cryptographie à des fins de confidentialité, la loi a introduit un système dit des « tiers confiance ». C'est à dire que l'utilisation de fonctions de confidentialité est libre, à condition que les conventions secrètes soient gérées selon les procédures et par un organisme agréé. Ce système existe seulement en France, il suscite d'ailleurs énormément d'interrogations, aussi bien juridique que technique.

La France est donc le seul pays de l'Union européenne à disposer d'une législation restreignant le libre usage de la cryptographie. « Depuis la loi du 29 décembre 1990, elle tolère tout au plus le cryptage de la signature et de la certification d'intégrité des messages, sur déclaration préalable auprès d'un service du Premier ministre, mais ne permet pas le chiffrement du message lui-même, qui doit être transmis en clair. »[2] La législation française sur le chiffrement crée des atteintes aux principes de libre circulation des marchandises, des services et des personnes.

En effet, elle met en place une impossibilité de fait pour un ressortissant communautaire voyageant en France d'utiliser des produits de chiffrement autorisés dans son pays. De plus, elle établit un obstacle à la libre circulation des marchandises, puisqu'un produit librement commercialisé dans un autre pays de l'Union est soumis à autorisation pour pouvoir être fourni en France.

La loi française se trouve donc en contradiction avec la politique communautaire sur plusieurs points. La directive européenne sur le traitement des données à caractère personnel[3] requiert que les Etats membres protègent les droits et les libertés des personnes. Les régimes établis, en France, pour l'utilisation et la fourniture des moyens de prestations de cryptographie pourraient affecter l'application de cette directive, dans la mesure où selon la Commission « les moyens appropriés nécessaires pour sécuriser les données personnelles ne seraient pas disponibles en France. »

---

1. JO du 27 juillet 1996
2. Le Monde 15 mai 1996 p.14
3. Directive 95/46 du 24 octobre 1995 JOCE 23/11/95 L281/30

La législation française est évidemment justifiée par des motifs de sécurité nationale, de défense. Pour les états, une protection trop forte de l'information porte atteinte à leur sécurité et profite au crime organisé. Cette réglementation reste donc inspirée par une logique sécuritaire et ne prend pas suffisamment en compte les besoins en matière de cryptographie et ne semble pas remplir « le test de proportionnalité du droit européen ».

De plus d'autre réglementation serait tout à fait envisageable, comme l'énonce Paul Vidonne, dans un article paru dans le Monde du 15 mai 1996 : « Un système de contrôle a posteriori serait beaucoup plus simple et moins coûteux à mettre en place. La liberté de crypter, laissant aux seuls utilisateurs le choix des moyens, serait compensée par l'obligation de communiquer les systèmes et clefs de cryptage à la requête de toute autorité judiciaire. Le refus explicite de communiquer serait très sévèrement réprimé, comme la perte ou l'oubli des clefs, qui serait présumés de mauvaise foi. Les pays qui ont mis en place un tel contrôle ne connaissent pas de criminalité particulière au regard de la communication. La France peut encore montrer qu'elle sait imaginer des réformes libérales, économiques et utiles. »

CONCLUSION

La surveillance électronique suscite beaucoup d'interrogations et soulève des objections, car le respect des droits fondamentaux est devenu le mot d'ordre de notre société. Une lourde tâche attend donc le Parlement européen, si celui-ci s'engage dans une lutte en faveur du respect de la confidentialité.

Permettre le secret des correspondances, c'est respecter la vie privée des utilisateurs, mais aussi créer un climat économique plus serein.

Le rôle du Parlement européen s'accroît, une meilleure coopération avec la Commission est d'actualité, puisque les nouveaux membres et le nouveau président de celle-ci , Romano Prodi (approuvés par le Parlement le 15 septembre 1999), l'ont promis. Ainsi le Parlement pourra imposer sa position notamment concernant le sujet qui nous intéresse car, comme nous l'avons vue, il a souvent été laissé de côté lors de prise de décision (exemple la résolution du 17 janvier 1995 du Conseil sur les interceptions légales).

L'étude, demandée à la STOA par la commission des Libertés Publiques et des affaires intérieures[1], et que nous avons présenté, lui expose les différentes options que le Parlement peut suivre pour essayer d'améliorer la réglementation en vigueur et établir une réelle sécurité des télécommunications.

---

1. Depuis juillet 1999 elle est dénommée: la Commission des libertés et des droits des citoyens, de la justice et de affaires intérieures.

ANNEXE :

DEFINITIONS :

- La confidentialité : elle permet de rendre la lecture de l'information inintelligible à des tiers non autorisés lors de sa conversation ou surtout de son transfert. Le chiffrement des informations constitue la technique la plus utilisée pour répondre à ce service.

- Le respect de la vie privée ; la liberté individuelle : c'est la protection de l'environnement de l'individu sur le plan de l'information, c'est à dire le droit de l'individu de contrôler ou d'agir sur des informations qui peuvent être collectées et stockées.

- La cryptologie : est un ensemble des techniques qui permettent de protéger les informations grâce à un code secret. Elle étudie notamment les outils servant à sécuriser ces informations face à des menaces institutionnelles. Ces outils sont généralement issus de problèmes mathématiques très difficiles à résoudre si l'on ne dispose pas de ce code. Elle permet la mise en œuvre des services de sécurité qui ont pour objectif de protéger des données ou des transactions sous forme électronique.

- La tierce partie de confiance : Une tierce partie de confiance est un organisme qui a la confiance de l'utilisateur et qui effectue, pour le compte de celui-ci, certaines opérations liées à la gestion des clefs de confidentialité. Il convient de distinguer les fonctions de tiers séquestre (des clefs servant à la confidentialité) et les fonctions d'autorité de certification pour des clefs publiques n'intervenant que dans des applications liées à la signature numérique.

- Signature numérique : elle est une technique qui permet la mise en œuvre à la fois de l'intégrité des données, de l'authentification et de la non-répudiation.

RESOLUTION DU 16 SEPTEMBRE 1998 :

Résolution sur les relations transatlantiques [système Echelon] --Paragraph 001

Le Parlement européen,
-.....vu sa résolution du 15 janvier 1998 sur les relations économiques et commerciales transatlantiques [JO C 34 du 2.2.1998, p. 139.] , -.....vu la communication de la Commission au Conseil, au Parlement européen et au Comité économique et social sur un nouveau marché transatlantique, -.....vu les conclusions du sommet États-Unis - Union européenne qui s'est tenu à Londres le 18 mai 1998, A.....considérant l'importance que revêtent la défense et le partage de valeurs communes à l'ère de la mondialisation, B.....considérant que les relations transatlantiques sont les plus intenses du monde, tant sur le plan politique qu'économique, C.....considérant que la progression et le renforcement des relations États- Unis - Europe auront pour effet d'accroître la stabilité politique et économique,

D.....rappelant que s'agissant des effets extraterritoriaux des lois Helms- Burton et d'Amato, le Parlement a adopté une position très ferme, E.....eu égard à l'étude intitulée 'évaluation des technologies de contrôle politique', rédigée par l'unité STOA [évaluation des choix scientifiques et techniques] pour la commission des libertés publiques; 1..... insiste sur l'importance des relations Etats-Unis - Union européenne, basées sur une communauté d'intérêts dans les domaines de l'économie, de la politique et de la sécurité, ainsi que sur une perception commune des responsabilités et des besoins au niveau mondial; 2..... considère que parmi ces objectifs politiques communs figure la promotion de la paix, de la stabilité, de la démocratie et du développement, ainsi que la volonté de faire face à des défis d'envergure mondiale au moyen d'une coopération renforcée; 3..... rappelle que les relations économiques transatlantiques reposent sur les liens économiques et commerciaux les plus importants du monde, et que l'Union européenne et les Etats-Unis entretiennent les rapports économiques les plus vastes et les plus complexes du monde; 4..... se félicite des résultats remarquables obtenus dans le cadre du nouvel agenda transatlantique [NAT], ce dont fait état la déclaration adoptée lors du sommet Etats-Unis - Union européenne susmentionnée; estime que dans ce contexte, le partenariat économique transatlantique [PET] constituera un instrument clé dans la progression des rapports bilatéraux; 5..... considère que le prochain accord, qui sera négocié dans le cadre du PET et portera en particulier sur les accords de reconnaissance mutuelle [ARM] et les 'normes équivalentes', sur les marchés publics et la propriété intellectuelle, devrait avoir pour effet de réduire considérablement les litiges à caractère bilatéral sur des questions de réglementation, et donner lieu à un processus de 'convergence en matière de réglementation'; 6..... encourage l'initiative 'People-to-People links' [liens entre les peuples] qui, en promouvant les contacts dans le monde des affaires, contribue de manière appréciable à démanteler les barrières existant dans le commerce transatlantique; 7..... insiste toutefois sur le fait que la législation extraterritoriale des Etats-Unis, et en particulier les lois Helms-Burton et d'Amato, demeurent inacceptables aux yeux de l'Union européenne; demande au Congrès des Etats- Unis d'intervenir rapidement en vue d'abolir de telles lois et, en tout état de cause, d'accorder les dérogations requises; 8..... demande à être tenu informé dans le détail des implications de l'accord dans la perspective de futures négociations sur l'AMI, dans la mesure où cet accord codifie certains des principes de base du projet AMI, tels que l'expropriation et la compensation; 9..... accueille favorablement la déclaration commune faite par la délégation pour les relations entre le Parlement européen et le Congrès des États-Unis sur le renforcement du dialogue interparlementaire en vue de l'instauration d'un partenariat transatlantique équilibré et bénéfique pour les deux parties; considère dès lors que les échanges s'inscrivant dans le cadre interparlementaire devraient être considérablement renforcés; 10..... est conscient du rôle crucial que joue la coopération internationale, grâce aux moyens de surveillance électronique, lorsqu'il s'agit de mettre un terme ou d'empêcher les activités des terroristes, des trafiquants de drogue et du crime organisé; 11..... reconnaît toutefois également qu'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 obtenues;

Paragraph 002

12..... demande que de telles technologies de surveillance fassent l'objet d'un réel débat ouvert, tant au niveau national qu'à celui de l'Union européenne, et soient soumises à des procédures garantissant une responsabilité sur le plan démocratique; 13..... réclame l'adoption d'un code de conduite destiné à garantir la réparation d'erreurs ou d'abus; 14..... estime que l'importance croissante du réseau Internet, et, plus généralement, des télécommunications à l'échelle mondiale et en particulier le système Echelon, ainsi que les risques de leur utilisation abusive appellent l'adoption de mesures de protection des informations économiques et d'un cryptage efficace; 15..... charge son Président de

transmettre la présente résolution à la Commission, au Conseil et au Congrès des États-Unis.
----------End of text

BIBLIOGRAPHIE :

Conventions internationales et textes de droit originel communautaire :

- La Déclaration Universelle des Droits de l'Homme 10 décembre 1948
- La Convention Européenne des Droits de l'Homme 04 novembre 1950
- La convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement des données à caractère personnel
- L'accord de WASSENAAR du 19 décembre 1995

- Le Traité de Rome du 25 mars 1957
- Le Traité d'Amsterdam du 02 octobre 1997

Textes de droit dérivé communautaire :

- Déclaration commune de l'assemblée du Conseil et de la Commission du 05 avril 1997 JOCE C103 24/07/1977
- Proposition de résolution du Parlement PE2-363/84
- Livre blanc de la Commission PE 115-274/déf
- Résolution du Parlement du 12 avril 1989 JOCE C120 du 16 mai 1989 p.51
- Directive 95/46/CE
- Directive 97/66/CE
- Résolution du Conseil du 17 janvier 1995 JOCE C329 04/11/1996 p.1 à 6
- Rapport PE 229/986/déf
- Résolution du 16 septembre 1998 JOCE 12/10/1998 C313 p.98
- Règlement 3381/94
- Proposition de règlement COM(98)257final
- Proposition modifiée de directive COM(99)195final
- Rapport PE 228.030/déf

Différentes publications :

- Le Monde diplomatique mars 1999
- Le Monde 15 mai 1996 p.14
- « Cryptographie : pourquoi faut-il libéraliser totalement la loi française ? » Valérie SEDALLIAN (http://wwwiris.sgdg.org/)
- « Une évaluation des techniques de contrôle politique » STOA PE 166.499 14/09/1998 (accessible sur le site de la STOA http:wwweuroparl.ep.ec/)
- « La législation française en matière de cryptologie » http://www.internet.gouv.fr

Autres documents :

- « Droit communautaire et protection des droits fondamentaux dans les Etats membres » Louis Dubouis édition Economica 1995
- « Affirmation des droits fondamentaux dans l'Union européenne » Commission européenne 1999
- « Aspect européen des droits fondamentaux » Gérard Cohen-Jonathan – préparation au CRFPA- édition MONTCHRETIEN 1996
- « Informatique et liberté » Henri Delahai édition la découverte 1987
- « La protection de la vie privée et les autres biens de la personnalité » François Rigaux édition LGDJ 1990
- « Droit de l'homme : repère juridique européen édition du Conseil de l'Europe janvier 1999
- « Tous concernés » édition du Conseil européen décembre 1998
- « Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel » publication officielle des Communautés européennes 1998
- « Services en ligne et protection des données et de la vie privée » publication officielle des Communautés européennes 1998 (volume1)
- « La jurisprudence de la Cour Européenne des Droits de l'Homme » V. Berger édition SIREY 1994