N° 2623

___

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

ONZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES(1),

sur ***les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale,***

et présenté par

M. Arthur PAECHT,

Député.

___

(1) La composition de cette commission figure au verso de la présente page.

Défense.

La commission de la défense nationale et des forces armées est composée de :

M. Paul Quilès, *président* ; MM. Didier Boulaud, Jean-Claude Sandrier, Michel Voisin, *vice-présidents* ; Robert Gaïa, M. Pierre Lellouche, Mme Martine Lignières-Cassou, *secrétaires* ; MM. Jean-Marc Ayrault, Jacques Baumel, Jean-Louis Bernard, André Berthol, Jean-Yves Besselat, Bernard Birsinger, Jacques Blanc, Loïc Bouvard, Jean-Pierre Braine, Philippe Briand, Jean Briane, Marcel Cabiddu, Antoine Carré, Bernard Cazeneuve, Guy-Michel Chauveau, Alain Clary, François Cornut-Gentille, Charles Cova, Michel Dasseux, Jean-Louis Debré, François Deluga, Claude Desbons, Philippe Douste-Blazy, Jean-Pierre Dupont, François Fillon, Christian Franqueville, Yves Fromion, Yann Galut, René Galy-Dejean, Roland Garrigues, Henri de Gastines, Bernard Grasset, Jacques Heuclin, François Hollande, Jean-Noël Kerdraon, François Lamy, Claude Lanfranca, Jean-Yves Le Drian, Georges Lemoine, François Liberti, Jean-Pierre Marché, Franck Marlin, Jean Marsaudon, Christian Martin, Guy Menut, Gilbert Meyer, Michel Meylan, Jean Michel, Jean-Pierre Michel, Charles Millon, Charles Miossec, Alain Moyne-Bressand, Arthur Paecht, Jean-Claude Perez, Robert Poujade, Michèle Rivasi, Michel Sainte-Marie, Bernard Seux, Guy Teissier, André Vauchez, Emile Vernaudon, Jean-Claude Viollet, Aloyse Warhouver, Pierre-André Wiltzer.

Sommaire

—

Pages

MESDAMES, MESSIEURS,

A la suite de la parution de plusieurs rapports du Parlement européen sur le réseau Echelon et d'interrogations de l'opinion publique reflétées par la presse à l'automne 1999, la Commission de la Défense nationale a décidé, le 29 février dernier, de confier à un de ses membres un rapport d'information sur les « systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale ». La Commission a également décidé d'associer aux activités du rapporteur d'information un groupe de travail dans lequel chaque groupe politique serait représenté.

Votre Rapporteur a été amené à s'interroger principalement sur plusieurs thèmes de réflexion :

— il a tout d'abord voulu comprendre la nature exacte du réseau Echelon, analyser ses capacités réelles et estimer ses véritables dangers (notamment à l'égard des enjeux de sécurité et d'une utilisation à des fins économiques). A ce titre, il a essayé de comprendre les moyens techniques dont les services de renseignement peuvent disposer pour recueillir l'information, la traiter et la diffuser ;

— il s'est ensuite interrogé sur les raisons de la « médiatisation » actuelle du réseau dit Echelon c'est à dire de l'intérêt subit pour les réseaux d'écoutes. Pour l'expliquer, il a donc cherché à savoir s'il n'y avait pas des raisons complexes s'apparentant par exemple à des manipulations ;

— il a également souhaité comprendre l'attitude des gouvernements occidentaux non membres du pacte fondateur d'Echelon, d'une part à l'égard des réseaux d'interception, d'autre part sur l'éventualité d'une coopération européenne des services d'écoute des communications ;

— enfin, il a cherché quels moyens permettraient de réduire la vulnérabilité des administrations, des services publics, des sociétés et des particuliers aux interceptions de leurs communications. Il s'est ainsi demandé quelle forme pourrait prendre une collaboration permettant aux Etats de l'Union européenne d'adopter une position commune face aux intrusions manifestes qui peuvent léser leurs intérêts.

L'objet de la mission d'information a été considéré comme difficile par tous les interlocuteurs rencontrés par votre Rapporteur, certains se félicitant cependant de l'intervention du Parlement et considérant que tout débat sur un tel sujet était sain. Les difficultés les plus importantes ont concerné les rencontres que votre Rapporteur a souhaité avoir avec les responsables des services de renseignement. En France, le ministère de l'Intérieur a permis à votre Rapporteur de rencontrer deux responsables de la Direction de la sécurité du territoire dont le directeur lui-même et le ministère de la Défense a accepté une audition du directeur général de la sécurité extérieure. De plus, la Délégation générale à l'armement a présenté à votre Rapporteur certains de ses chercheurs dans le domaine des écoutes.

A l'étranger, votre Rapporteur s'est heurté à une fin de non-recevoir de la part des autorités américaines et britanniques.

Il est tout d'abord intéressant de souligner que le refus des Britanniques s'est fondé sur le fait que votre Rapporteur n'était « *même pas membre d'une délégation parlementaire chargée du contrôle des services de renseignement* ». Cette attitude ne peut que conforter la Commission de la Défense dans l'idée que l'inscription de la proposition de loi visant à la création d'une telle structure à l'ordre du jour de l'Assemblée nationale est plus que jamais nécessaire.

Aux Etats-Unis, les réticences de l'administration, malgré les relances répétées de notre Ambassade à Washington, sont difficilement compréhensibles. Il a été expliqué qu'il ne s'agissait pas d'une commission d'enquête mais d'une mission d'information venant recueillir l'avis des responsables américains. Le refus de recevoir votre Rapporteur, pris semble-t-il au plus haut niveau après de nombreuses délibérations, a comme conséquence de relancer toutes les suspicions sur le rôle d'Echelon et des Etats-Unis en particulier. Il est d'autant plus surprenant que des responsables ou d'anciens responsables d'agences fédérales se sont exprimés publiquement sur le sujet. L'ensemble des interlocuteurs rencontrés à Washington a d'ailleurs exprimé son incompréhension vis-à-vis de ce refus.

L'objectif du rapport d'information n'a donc pu être, dans un premier stade, que d'apporter des précisions sur les capacités d'un système d'écoutes international nommé Echelon, d'en évaluer les risques à l'égard de la sécurité nationale et de formuler quelques propositions qui visent avant tout à protéger les acteurs français de l'interception de leurs communications.

Les conclusions risquent d'apparaître à certains très en retrait par rapport aux conséquences des écoutes sur les libertés individuelles et l'indépendance des Etats.

Mais le travail effectué n'a aucune vocation polémique. Celle-ci serait d'ailleurs inutile voire néfaste dans un domaine où il est apparu extrêmement difficile d'obtenir des renseignements et de les vérifier, et où coopèrent les services de renseignement des membres de l'Alliance atlantique.

I. — Le système Echelon : une réalité dont les conséquences sont difficiles à apprécier

Ne souhaitant pas effectuer une analyse exhaustive des systèmes d'interception des communications, votre Rapporteur a préféré tenter de répondre à quelques questions qui lui paraissaient fondamentales : quelles sont les véritables finalités de ces systèmes et en particulier d'Echelon ? Quelles sont ses capacités réelles ? Pourquoi l'existence de tels réseaux a-t-elle pris récemment une importance médiatique sans commune mesure avec le passé ? Quelles peuvent être les réactions des pays occidentaux qui peuvent être victimes de ces interceptions tout en étant quelquefois partie prenante ?

A. Une organisation vraisemblablement détournée de sa finalité militaire initiale

Bien que de nombreux articles et ouvrages aient déjà évoqué l'existence et l'organisation d'un système nommé Échelon, il paraît nécessaire d'en rappeler les grandes caractéristiques, non seulement en raison de l'importance du phénomène, mais aussi de ses conséquences pour les intérêts politiques et économiques des pays européens.

L'évolution du système depuis sa création est révélatrice de la prédominance de l'acteur principal que sont les Etats-Unis et de leur souhait que l'ensemble des pays occidentaux alignent leur politique d'écoutes sur la leur.

1. Le développement du réseau dans un contexte de guerre froide

a) Un pacte initial marqué par le contexte historique

L'un des maillons essentiels de la stratégie de *containment* des Etats-Unis à l'égard du pacte de Varsovie a consisté à créer un pacte de sécurité destiné à intercepter les communications politiques et militaires du bloc soviétique. Héritier d'un système américano-britannique en vigueur pendant la seconde guerre mondiale, ce pacte secret, signé au départ en 1947 par les Etats-Unis et le Royaume-Uni, d'où son nom UKUSA, a été élargi à trois pays, d'abord le Canada qui aurait conclu un accord bilatéral avec les Etats-Unis (CANUSA *Agreement*), la Nouvelle-Zélande et l'Australie.

Le choix de ces anciennes colonies britanniques ne doit rien au hasard puisque les stations d'écoutes, progressivement installées sur leurs territoires, ont permis une couverture quasimondiale et ont facilité l'interception des communications de l'URSS et de ses satellites, voire de certains Alliés comme la France.

Dans la théorie du renseignement, le pacte UKUSA permet de développer une nouvelle forme de renseignement, le COMINT (*communications intelligence*) complémentaire des autres gammes existantes et en englobant d'ailleurs certaines : HUMINT (*human intelligence* ou renseignement d'origine humaine), ELINT ou SIGINT (*electronic intelligence* ou *signal intelligence* c'est-à-dire renseignement d'origine électronique), RADARINT (*radar intelligence*).

Le pacte peut être interprété de deux manières :

— soit comme la traduction du partage géographique des tâches entre les cinq participants dont chacun, par le biais de ses services d'interception, doit collecter l'information à partir de ses propres stations d'écoute, traiter cette information et procéder à des échanges avec ses partenaires. Echelon constituerait alors le seul système multilatéral d'interception des communications dans le monde, tous les autres systèmes de coopération entre services ayant une nature bilatérale ;

— soit comme l'extension à un niveau mondial du système américain USSS (*United States Sigint System*) avec une logique coopérative inégale.

Le système fait donc appel aux services de renseignement spécifiques des cinq pays participants. Les indications sur les moyens humains et matériels de chaque service, données dans le tableau suivant, reflètent évidemment l'importance relative des participants.

Pays	Service d'interception	Effectifs	Moyens
Australie	Defense Signals Directorate DSD	n.d.	n.d.
Canada	Communication Security Establishment CSE	Environ 900	n.d.
Etats-Unis	National Security Agency NSA	40 000	4 milliards de dollars (budget 1997)
Nouvelle-Zélande	Government Communications Security Bureau GCSB	1 500	n.d.
Royaume-Uni	Government Communications Headquarters GCHQ	15 000	500 millions de livres

L'importance de la finalité militaire initiale du pacte mérite d'être soulignée dans la mesure où elle permet de replacer celui-ci dans le contexte géostratégique de son élaboration et où elle peut justifier que des relations aient pu se nouer entre le réseau ainsi constitué et d'autres services de renseignement, en particulier parmi les membres de l'Alliance atlantique.

Ainsi, les moyens d'écoute des Allemands et des Français installés sur le territoire de la RFA étaient-ils tournés en direction du Pacte de Varsovie et contribuaient-ils à renseigner l'OTAN durant toute la période de la guerre froide.

La finalité militaire est d'ailleurs l'argument invoqué pour le maintien du réseau après la disparition du Pacte de Varsovie.

D'une part, il semble légitime que les objectifs de sécurité, partagés par les pays occidentaux face aux nouvelles menaces communes que constituent par exemple le terrorisme international ou le développement des trafics de produits illicites, conduisent à des relations étroites des services nationaux en charge de la sécurité. Votre Rapporteur reviendra d'ailleurs sur ce point.

D'autre part, il a été indiqué à votre Rapporteur que les installations d'écoutes situées sur la base de Bad Aibling en Allemagne étaient utilisées à présent pour la surveillance des Balkans et avaient bénéficié à l'Alliance atlantique lors de ses interventions en ex-Yougoslavie depuis une dizaine d'années. Les responsables allemands rencontrés par votre Rapporteur partagent l'analyse des Etats-Unis qui continuent à

soutenir que les systèmes d'interception des communications ont une finalité militaire, après le temps de la guerre froide.

b) Un développement spectaculaire qui a suivi celui des technologies

Le véritable développement du système date des années 70. Il est lié aux progrès technologiques dans les domaines des communications (recours aux satellites), des moyens d'écoute (paraboles et radômes) et du traitement des données par les systèmes informatiques. C'est en effet à partir de cette période que les ordinateurs sont devenus capables de trier les données grâce à des systèmes de mots-clés et que des connexions ont permis de relier les outils informatiques des différents partenaires, facilitant ainsi le traitement et les échanges d'information.

Comme dans le cas de tout système de renseignement, le fonctionnement du réseau Echelon comporte en effet trois phases : l'écoute des télécommunications, le traitement des informations recueillies et l'échange des données.

Les méthodes d'écoute concernent tous les vecteurs utilisés pour les communications modernes : ondes radio, satellites, câbles terrestres ou sous-marins, fibres optiques, réseaux informatiques…

L'interception des communications qui transitent par satellite s'opère au moyen de stations d'écoutes au sol. Certaines sont dédiées au réseau de satellites Intelsat utilisés par la plupart des opérateurs occidentaux, d'autres aux satellites Immarsat dont la vulnérabilité a été soulignée. La croissance des communications transitant par Intelsat a contraint les membres de l'UKUSA à augmenter le nombre de leurs stations d'écoutes. A celles de Morvenstow au Royaume-Uni et de Yakima aux Etats-Unis se sont ajoutés les sites de Chum Hom Kok, près de Hong-Kong, Sugar Grove près de Washington, Waihopai en Nouvelle-Zélande (depuis 1989) et Geraldton en Australie (depuis 1993). D'autres stations sont orientées vers les satellites de communications régionales et connectées aux satellites américains espions dont plusieurs générations ont été lancées en orbite depuis le début des années 60.

Le document transmis au Parlement européen « *Interception Capabilities 2000* » estime que les nations participant au réseau Echelon disposent en permanence de 120 satellites espions pour les seuls échanges qui transitent par l'espace.

La réception des données recueillies par les satellites et les stations d'écoute est effectuée par des stations au sol basées aux Etats-Unis, en

Grande-Bretagne (Menwith Hill) et en Australie (Pine Grap) mais également au Canada (Letrin près d'Ottawa), en Allemagne (Bad Aibling) ou au Japon (Misawa).

L'une des plus grandes difficultés consiste à extraire, de la masse des messages recueillis (plus de trois millions par minute dans le monde selon certains experts), ceux qui comportent un réel intérêt.

La technique utilisée repose sur l'utilisation de mots-clés préalablement sélectionnés et répertoriés dans des dictionnaires. Chaque agence de renseignement élabore ainsi des listes de mots selon les activités qu'elle souhaite suivre et contrôler. Les mots-clés correspondent par exemple à des noms de dirigeants politiques ou économiques, d'entreprises, d'institutions, de produits ou de références de répertoires (adresses, numéros de téléphones, de télex ou de fax). Pour éviter d'être submergé par la masse des données, le système est capable d'élaborer des combinaisons de mots-clés qui sont elles-mêmes indexées dans les dictionnaires. Les dictionnaires des ordinateurs sont interconnectés. Chaque système a en mémoire des listes de mots-clés ou des combinaisons de chaque agence nationale -mais pas forcément l'ensemble des listes ou des combinaisons du système-, ce qui lui permet de repérer les messages contenant ces mots-clés et de les transmettre à l'agence concernée. La mise à jour des dictionnaires est quotidiennement assurée par chacune des agences intéressées.

Le système implique que les messages triés soient analysés. Ceux qui ne sont pas en langue anglaise sont traduits ce qui suppose des équipes de traducteurs très nombreuses. Les messages qui présentent un intérêt sont synthétisés sous forme de rapports au standard déterminé et envoyés « à certaines parties du réseau Echelon ».

Une difficulté récente pour le système provient du développement des méthodes de cryptage utilisées par les plus grands groupes industriels ou certains services étatiques pour assurer la confidentialité de leurs communications. Une des explications apportées à la diffusion récente d'informations sur le réseau Echelon est liée à la difficulté croissante des services d'écoute face au développement de la cryptologie et à la nécessité pour ces services de suivre les progrès des technologies dans ce domaine et d'éviter que celles-ci n'empêchent une action qu'ils considèrent légitime. Ce point sera développé dans une seconde partie du rapport.

Le développement du réseau Echelon a été multiforme. Tout d'abord, le système n'a pas été conçu pour intercepter seulement certains types de communications comme les messages à caractère militaire lors de la guerre froide, mais il a eu vocation à intercepter de manière indistincte

tous les messages dans le monde, quels que soient la nature de leur support et leur contenu, c'est-à-dire y compris les communications privées. Sont donc concernés tous les messages transmis par écrit (télex, fax, plus récemment courrier électronique) et par ondes hertziennes. Depuis le développement des téléphonies mobiles et le recours aux satellites, ce sont également les communications « vocales » qui sont susceptibles d'être interceptées.

c) Un partenariat à plusieurs niveaux

La conviction de la mission d'information est double : non seulement, les Etats-Unis jouent un rôle prépondérant et dirigeant dans le système, mais les autres partenaires sont dans une situation qui reflète à la fois leur dépendance et leur sujétion.

La suprématie américaine à l'égard des réseaux d'écoute et d'interception se fait sentir sur de nombreux plans.

Tout d'abord, l'architecture du réseau Echelon a été entièrement conçue par la NSA en charge statutairement du renseignement électronique SIGINT et les quatre autres agences nationales n'ont fait que l'adopter. Seule la NSA dispose de l'ensemble des codes ou combinaisons et a l'accès à l'ensemble du réseau. Les agences non américaines doivent obtenir l'autorisation de la NSA pour, par exemple, s'abonner à des dictionnaires et recevoir des informations des stations qu'elles ne contrôlent pas.

L'une des questions les plus intéressantes à propos d'Echelon porte sur le degré d'intégration des différents services de renseignement. Il est difficile de connaître la logique interne du système car les contacts bilatéraux entre services qui permettraient une telle analyse ne sont pas aussi prononcés que les médias l'imaginent. Echelon pourrait à cet égard être qualifié de coopérative inégalitaire, les « associés » se trouvant dans des situations différenciées.

Les Etats-Unis constituent le maître d'œuvre de l'ensemble. Le Royaume-Uni, en raison de ses compétences et d'une longue tradition, est un partenaire privilégié. Les trois autres pays sont dans une situation d'associés plutôt que de partenaires : ils ont un rôle assigné en termes de technologies et de secteurs d'intervention en raison d'un moindre niveau de leurs capacités d'interception. Toutes les informations recueillies sont communiquées à la NSA de manière automatique mais ne sont redistribuées aux autres agences que si la NSA l'estime nécessaire. Il semble aussi que, si un pays introduit un mot-clé qui l'intéresse particulièrement dans le dictionnaire des ordinateurs du système, la NSA soit forcément au courant

que les informations contenant ce mot-clé sont communiquées au pays demandeur.

Le cas de la Nouvelle-Zélande est symptomatique puisque le refus de ce pays d'accepter des navires nucléaires américains dans ses ports et ses réticences face au système semblent l'avoir marginalisé dans un premier temps, les Etats-Unis prenant des mesures de rétorsion, voire exclu d'un second réseau plus intégré des agences de renseignement et relatif aux échanges d'informations après traitement. Mais la Nouvelle-Zélande continue à participer au réseau et les échanges entre services ont été maintenus. Ils ont été actifs pendant la dernière campagne d'essais nucléaires de la France dans le Pacifique compte tenu de la situation géographique de la Nouvelle-Zélande.

2. Un réseau détourné de sa vocation initiale

Alors que la disparition du Pacte de Varsovie et l'effondrement du bloc soviétique auraient pu amener le système global d'interceptions des communications à disparaître, il semble qu'avant même la fin des années 80, Echelon ait été orienté à d'autres fins, y compris le renseignement économique, voire utilisé avec des objectifs politiques entre Alliés.

a) La possibilité d'utilisation des écoutes à des fins économiques

L'utilisation des services officiels de renseignement pour promouvoir les activités économiques est une réalité. C'est à la fois une tentation permanente et une conséquence inévitable de l'activité de ces services, au-delà de toutes leurs dénégations.

De nombreux exemples ont été fournis par les médias pour illustrer le dévoiement d'un système d'interception des communications comme Echelon. Ils concernent des négociations internationales aussi bien politiques qu'économiques. Ils visent, soit des Etats ou des institutions internationales (OMC ou Union européenne), soit des entreprises, notamment celles en concurrence avec des groupes américains sur des marchés tiers : les exemples les plus couramment cités concernent Thomson-CSF contre Raytheon pour un marché de radars au Brésil, Airbus contre Boeing en Arabie Saoudite, ou la firme allemande Siemens pour un marché d'électronique en Inde.

L'orientation des services de renseignement des Etats-Unis vers un soutien direct à la politique commerciale de leur pays n'est pas nouvelle. L'administration américaine sous la présidence de Bill Clinton a clairement

exprimé le choix d'une intervention croissante de l'exécutif et des services gouvernementaux en faveur du secteur industriel. La création du *National Council of economy* répond au même objectif de défense des intérêts économiques des Etats-Unis par tous les moyens.

Depuis quelques années, le gouvernement américain a reconnu une capacité d'interception des télécommunications à partir d'un système militaire d'écoutes qui s'est diversifié. L'élément nouveau est qu'à la suite du premier rapport au Parlement européen de son service d'études (STOA) en 1998, certains responsables officiels américains ont fait de multiples déclarations pour justifier le réseau Echelon en avançant deux raisons majeures : le développement de pratiques commerciales déloyales de la part des Européens et notamment des Français (argument économique de moralité) et l'existence de capacités similaires d'interception dans d'autres pays européens, en particulier en Allemagne et en France.

Les présentations de M. Michael V. Hayden, directeur de la NSA, ou de M. George J. Tenet, directeur de la CIA, devant les membres du Congrès, et en particulier leurs auditions à plusieurs reprises devant les deux commissions spéciales en charge du renseignement à la Chambre des représentants et au Sénat, s'appuient souvent sur l'énoncé de grands principes moralisateurs :

— d'une part, les deux responsables des agences fédérales ont toujours soutenu que les activités des services de renseignement étaient compatibles avec les « *lois des Etats-Unis et les droits fondamentaux des citoyens américains* ». Ils ont ainsi affirmé qu'aucune conversation privée de citoyens américains ne faisait l'objet d'écoutes. Ils ont rappelé que l'activité des services de renseignement était strictement encadrée par des mécanismes législatifs et réglementaires, dont l'Executive order n° 12-333, que ces activités devaient être approuvées par l'Attorney General, que les agents des services de renseignement étaient tenus de dénoncer les violations qu'ils pouvaient constater, et que les Inspecteurs généraux des services de renseignement (CIA, DIA, FBI ou NSA) faisaient rapport au Président des Etats-Unis des activités qu'ils estimaient illégales ;

— d'autre part, trois objectifs semblent avoir été fixés aux services de renseignement américains : surveiller les entreprises qui rompent les embargos décidés par l'ONU ou les Etats-Unis, suivre les technologies duales pour éviter leur utilisation dans la production d'armes de destruction massive, moraliser le commerce international et éviter ainsi que les entreprises américaines ne soient pénalisées par les comportements délictueux de leurs concurrents.

Les affirmations des responsables des agences fédérales doivent être relativisées au regard des considérations suivantes :

— plusieurs exceptions permettent aux agences fédérales américaines d'écouter les conversations privées, notamment le soupçon qu'une personne travaille pour un « pouvoir étranger », l'existence d'un mandat d'une cour de justice ou le fait que les communications se déroulent en dehors du territoire américain (*overseas*). En outre, les autorités fédérales auraient la possibilité de conserver des conversations au-delà du délai légal de 24 heures en dehors du territoire américain, donc de les exploiter même lorsqu'elles ont été réalisées par des citoyens américains ;

— des structures de coordination existent pour favoriser les échanges entre le secteur privé et les administrations américaines. Ces échanges ont bénéficié depuis quelques années d'un transfert mutuel de personnels. La CIA a embauché de plus en plus de jeunes disposant déjà d'une première expérience professionnelle dans le secteur privé. La NSA et la CIA ont encouragé la reconversion d'une partie de leur personnel vers le secteur privé. Les responsables des services informatiques et de sécurité des entreprises sont souvent d'anciens employés des agences fédérales ;

— les méthodes mises en œuvre pour contrôler certaines activités sont similaires à celles visant l'espionnage économique. Comme le reconnaissent plusieurs membres du Congrès, il est quasiment impossible de séparer ces activités. Le directeur de la CIA affirme que l'agence intervient lorsqu'une entreprise américaine pourrait être «lésée» dans ses intérêts par un concurrent ne se conformant pas à des pratiques loyales. Les informations sont transmises aux ministères intéressés (Treasury Department, Commerce Department, Justice Department,…) qui peuvent alors décider d'avertir ou non l'entreprise concernée.

Les propos tenus par les actuels dirigeants des agences fédérales en charge du renseignement rejoignent ceux de M. R. James Woolsey, ancien directeur de la CIA. Dans deux articles, aux tons d'ailleurs assez divergents mais empreints d'ironie et provocateurs, il a reconnu que des écoutes avaient été effectuées aux dépends d'entreprises européennes. Il les a justifiées au nom de la lutte contre la corruption et de la croisade contre le versement de « *pots-de-vin* » par les groupes européens à des Gouvernements tiers.

Lors de son audition, M. R. James Woolsey s'est tout d'abord défendu d'avoir affirmé que les Etats-Unis faisaient actuellement de l'espionnage économique aux dépens de sociétés étrangères. Il a affirmé que

le titre du Wall Street Journal employant le présent (« *Why we spy our Allies ?* ») était dû aux journalistes et non à lui-même. Il a par contre admis que, lorsqu'il était directeur de la CIA, certaines écoutes concernaient des entreprises soupçonnées de verser des pots-de-vin. Il a rappelé que 95 % des informations provenaient des ressources ouvertes et seulement 5 % des sources secrètes sur des sujets déterminés. Aux Etats-Unis, la communauté du renseignement a toujours fait du renseignement économique pour trois raisons (suivi des biens à double usage, respect des sanctions économiques, utilisation de méthodes frauduleuses de la part d'entreprises ou de gouvernements étrangers). Il n'a jamais été question de recueillir des secrets technologiques au profit d'entreprises américaines.

M. R. James Woolsey a également indiqué que lorsqu'il était directeur de la CIA, des sénateurs l'avaient interrogé pour savoir s'il était prêt à engager l'agence vers l'espionnage industriel. Certains journalistes ont interprété sa réponse comme un soutien aux entreprises américaines. Mais plusieurs analystes ont conclu que jamais le Gouvernement américain n'autoriserait la participation d'une agence fédérale à de telles activités. De plus, les restructurations industrielles et la globalisation des procédés au niveau mondial rendent difficile l'attribution d'une nationalité aux entreprises. Il est ainsi quelquefois impossible de savoir si on s'adresse à une société étrangère ou américaine. Aussi laquelle faudrait-il aider ?

Si la presse américaine avait pu relever des cas où les agences fédérales ont favorisé les entreprises américaines, elle aurait été ravie de dénoncer leur hypocrisie. La transparence du système serait telle qu'il est impossible que des détournements n'aient pas été connus. De plus, l'espionnage ne correspond pas à l'objectif primordial de sécurité et risquerait de détourner les capacités d'enjeux plus importants.

Le détournement à des fins économiques place d'ailleurs les autres pays dans des situations difficiles, notamment le Royaume-Uni. Les intérêts des Etats-Unis et du Royaume-Uni peuvent diverger, par exemple en matière de marchés d'équipements militaires ou d'aéronautique civile.

Or le Royaume-Uni participe à des interceptions dont les résultats peuvent être quelquefois utilisés contre les intérêts mêmes de ses entreprises nationales ou de sa politique extérieure. Le cas du marché perdu par le consortium Airbus est révélateur puisque le groupe British Aerospace détient 20 % de ce consortium.

De même, la présence du Royaume-Uni dans le système est encore plus préoccupante pour toutes les affaires relevant de l'Union européenne s'il s'avère que l'Union est « piégée » lors des négociations internationales

ou dans les sommets concourant à la réforme des institutions communautaires ou encore au développement de la politique européenne de sécurité et de défense.

b) Les réactions des industriels concernés par les écoutes

Aux questions qui leur ont été posées par la mission d'information, les réponses des industriels français ou allemands, potentiellement victimes d'écoutes, ont été concordantes.

Si les responsables de grands groupes ont généralement indiqué qu'ils étaient effectivement concernés par l'espionnage économique, qui était une réalité, ils ont cependant reconnu qu'il était difficile de connaître l'origine des fuites et qu'il leur était impossible d'affirmer que des marchés avaient été perdus en raison d'écoutes.

Pour les responsables américains, la perte de contrats par des sociétés européennes n'est pas due aux écoutes ni à l'espionnage de leurs secrets commerciaux mais aux versements de pots-de-vin. Lorsque les Etats-Unis ont eu connaissance de telles pratiques, dans un souci de moraliser le commerce international, ils ont demandé à leurs ambassadeurs d'intervenir auprès des responsables des pays acheteurs.

Pour les industriels, l'échec commercial peut tenir à de nombreux facteurs, surtout dans un contexte international. Aux considérations techniques et financières sur les programmes concernés, s'ajoutent dans de nombreux cas des préoccupations stratégiques. Il est vrai que certaines sociétés s'aperçoivent parfois, au cours des négociations et notamment dans les appels d'offres internationaux, que des concurrents ont eu connaissance des éléments de la négociation, ne serait ce qu'au travers des « offres sondes » qui sont envoyées et qui révèlent l'existence d'écoutes.

Il est ainsi intéressant de souligner qu'aucune plainte d'entreprise française, ou même européenne, n'a jamais été déposée en raison de dommages occasionnés par des écoutes électroniques, ce qui explique que le Quai d'Orsay n'ait jamais eu de réprobation diplomatique à formuler. Symétriquement, aucune entreprise américaine ne s'est jamais plainte d'écoutes de la part de services européens de renseignement. Les deux exemples les plus connus (Brésil et Arabie) ne prouvent pas que la NSA ait fourni des informations à des entreprises américaines mais les spécialistes estiment que la NSA est intervenue.

Par ailleurs, les demandes accrues des sociétés, dont les enjeux économiques sont devenus internationaux, pour des réseaux cryptés de communication témoignent de la crainte de subir des attaques et de la prise

de conscience de l'intérêt de se protéger contre les intrusions.

Certaines réactions n'ont cependant pas été sans surprendre votre Rapporteur. Ainsi, un grand groupe multinational a souligné que les industriels ne pourraient ou ne voudraient pas répondre aux questions relatives au rôle d'Echelon, parce qu'eux-mêmes, dans certains cas, mettaient en œuvre leur propre réseau. Seuls les grands groupes peuvent mettre en place leurs propres structures de renseignement et les PMI-PME n'ont pas les capacités d'avoir leurs propres services d'intelligence économique, surtout celles qui ne sont pas filiales de grands groupes. Mais toute société peut faire appel à des entreprises spécialisées qui recherchent et exploitent l'information ouverte.

De plus, il faut être conscient de la multiplication des sociétés chargées de récupérer des informations au profit de tiers. Ces sociétés ont les compétences pour pénétrer dans les systèmes informatiques et utilisent les mêmes méthodes que les pirates sur le réseau Internet. Les opérateurs de réseaux effectuent une surveillance mais les réseaux comportent des failles qui sont utilisées par certains, même sur le territoire national.

B. L'incertitude sur les capacités réelles du système

Les experts consultés ou rencontrés par votre Rapporteur n'ont pas toujours tenu des discours concordants sur les capacités des réseaux d'interception des communications et du système Echelon en particulier.

1. La thèse maximaliste

Pour certains spécialistes, qui ont sans doute une **vision maximaliste,** le système mis en place est capable d'intercepter l'ensemble des communications au niveau mondial, quel que soit le réseau technique utilisé. Ils affirment que toutes les télécommunications par satellites sont interceptées, stockées et triées, et qu'il en est de même pour les communications filaires (téléphones fixes, fax). Pour eux, s'il existe, l'analyse en différé peut compenser, au moins en partie, certains manques dans les capacités immédiates de traitement.

Ces affirmations sont soutenues par la vulnérabilité des technologies de l'information et les progrès des techniques d'interception des communications, facteur clé du sujet.

a) La vulnérabilité des technologies de l'information

Il paraît nécessaire de souligner que tous les éléments composant

les technologies modernes de communications possèdent leurs propres vulnérabilités : les matériels (circuits intégrés, processeurs, …), les logiciels (programmes qui commandent les matériels), les supports de communication (câbles, fibres optiques, ondes radio, …).

Les systèmes d'information et de communications (SIC) sont vulnérables à l'écoute passive (écoute des signaux par interception des liaisons satellitaires ou des faisceaux hertziens, par branchement sur les réseaux filaires ou écoute des réseaux), aux intrusions (recherche de l'information au cours des interceptions GSM, attaques lors des télémaintenances, vols de session, usages de portes dérobées dans les systèmes d'exploitation,…) voire à l'écoute active (l'information est fournie par la source en raison de virus informatiques ou de chevaux de Troie introduits dans le système de l'émetteur). On peut même affirmer que les SIC deviennent de plus en plus vulnérables dans la mesure où l'émetteur d'un message ne contrôle plus le stockage et la communication de ses messages, et que la captation des traces laissées par ceux-ci est de moins en moins visible.

Les communications satellitaires peuvent facilement être interceptées en raison des liaisons entre les satellites géostationnaires et les stations au sol. Les rayonnements sont susceptibles d'être captés soit directement par des satellites espions, soit par des stations terrestres dont les antennes sont judicieusement dirigées. Il n'en est pas de même des réseaux filaires qui ne peuvent être piratés qu'en dehors du territoire national (sauf à disposer de complicités). Le cas des câbles sous-marins est illustré par Duncan Campbell qui cite l'intervention de sous-marins américains posant des manchons ou *pods* sur des câbles soviétiques et sur des câbles entre l'Europe et l'Afrique de l'Ouest.

La vulnérabilité des réseaux s'est accrue avec le développement de l'informatique. Dans ce contexte, le débat sur les écoutes ne peut manquer de s'étendre à la question des intrusions dans les réseaux, c'est-à-dire au plus près de la source émettrice du message, au cœur de l'architecture des réseaux.

Les intrusions utilisent toutes les failles des matériels (*hardwares)* et des logiciels *(softwares)*. De nombreux spécialistes ont confirmé ces failles à votre Rapporteur : elles peuvent prendre la forme de fonctions cachées dans les logiciels du commerce, c'est-à-dire non signalées dans la documentation remise à l'utilisateur mais qui peuvent être activées par un tiers. Certaines de ces fonctions sont anodines encore qu'il soit impossible de savoir si elles ne contiennent pas d'autres finalités que l'amusement de leur programmeur. Mais bien d'autres fonctions n'ont pas pu être détectées

et posent la question de programmes espions dits *back doors* dans les logiciels du commerce.

Les spécialistes de la DGA qui travaillent au centre d'électronique de l'armement (CELAR) à Rennes ont fait la démonstration à votre Rapporteur de l'existence de failles ou de fonctions cachées dans certains logiciels, et ont mené des attaques virtuelles contre des sites Internet en utilisant les anomalies de fonctionnement des logiciels et en prouvant par là que la guerre de l'information était devenue une réalité.

Depuis de nombreuses années, ces failles technologiques sont dénoncées par des chercheurs ou des spécialistes. Elles sont d'autant plus redoutables qu'elles émanent de produits d'origine américaine qui représentent près de 80 % du marché mondial. Certes, certaines sont involontaires mais d'autres ont été créées sciemment. Leur vocation est avant tout commerciale puisqu'une défaillance suppose d'être améliorée : les nouvelles versions des logiciels trouveront ainsi des débouchés commerciaux. On peut aussi supposer qu'elles ne sont pas toutes motivées par des préoccupations commerciales.

Si elle a reconnu l'existence de fonctions cachées dans ses produits, la société Microsoft a démenti à plusieurs reprises, non seulement qu'elle entretenait des liens avec les services de renseignement américains, mais que ses programmes permettaient de décoder les informations contenues dans les ordinateurs utilisant ses logiciels (par exemple Windows, Word ou Excel voire Internet Explorer).

Il est vrai que, face à la difficulté d'analyser les produits dont ils ne connaissent que la partie exécutable, les chercheurs restent réservés sur de telles possibilités.

Leur existence aurait cependant été confirmée au gouvernement français par un rapport « *Sécurité des systèmes d'information : dépendance et vulnérabilité* » de l'Amiral Jean Marguin commandé par la Délégation aux affaires stratégiques (DAS) du ministère de la Défense et remis début février 2000. Ce rapport, dont la presse a déjà fait état, analyserait les défauts des logiciels et les risques de collusion entre les agences fédérales et les sociétés créatrices de ces logiciels. Il insisterait sur les liens entre Microsoft et le Pentagone (son principal client dans le monde). Il chercherait également à expliquer la découverte réalisée en août 1999 par un chercheur canadien Andrew Fernandes qui identifia dans Windows une ligne de code faisant référence à la NSA.

Il faut cependant éviter de considérer que tous les produits sur le

marché ont fait l'objet de manipulations. D'une part, les entreprises américaines n'ont pas le monopole du marché, d'autre part, les services officiels n'ont pas les moyens de piéger tous les logiciels, enfin, les techniques de cryptage sont puissantes. De plus, alors que les entreprises de la défense et de l'espace, bien que privées, entretenaient des relations étroites avec le Gouvernement américain, en particulier avec le ministère de la défense (DoD), les sociétés productrices de logiciels sont plutôt hostiles à l'intervention de l'Etat et aux règles fédérales, elles sont plus indépendantes et ont moins la volonté de coopérer avec l'Etat, comme en témoignent les difficultés de Bill Gates, président de Microsoft, avec la justice.

b) Le débat sur les capacités techniques du système

Se fondant sur une comparaison des budgets des agences de renseignement, certains experts estiment que les capacités des agences américaines sont énormes et que toutes les déclarations officielles sur ces capacités n'ont eu de cesse de les minimiser.

Il faut rester prudent sur les potentialités des systèmes d'écoute et les chiffres fournis en termes de nombre de messages interceptés ne signifient pas grand chose. Tout d'abord parce que ce qui importe c'est la capacité de traitement. Ensuite, parmi la population, l'intérêt des services d'écoute est d'identifier les cibles qui comptent (environ 5 000 personnes par exemple en France) et de les suivre : les moyens d'écoute sont donc orientés sur les personnalités donc les communications les plus intéressantes.

Enfin, les sources ouvertes sont suffisantes pour fournir des bases de données. On peut ainsi suivre l'activité des sociétés et de leurs dirigeants à travers la presse spécialisée et technique.

Certains experts ajoutent que les écoutes fournissent des renseignements sur les caractéristiques d'un réseau de communications (architecture, rythme, localisation et déplacement des sources émettrices, intensité…) qui permettent de déterminer sa nature. L'exemple historique du réseau crypté soviétique A 12 détecté en Allemagne de l'Est est souvent cité à cet égard. Mais de nombreux exemples récents ont été cités, la simple existence de messages chiffrés entre deux personnes constituant déjà une information.

2. La thèse du scepticisme

Pour d'autres, **plus empreints de scepticisme**, de nombreux facteurs limitent les potentialités des systèmes d'écoutes comme Echelon :

— d'une part, il est douteux que l'ensemble de la planète soit couvert, le réseau Echelon par exemple ayant été constitué pour lutter contre le bloc communiste et ses satellites, et reposant en priorité sur l'interception des communications satellitaires ;

— d'autre part, les communications filaires restent difficiles à intercepter sans que l'utilisateur ne s'en aperçoive ou sans la complicité de l'opérateur de réseau (*a contrario*, de forts soupçons existent sur une connivence possible entre British Telecom et le GCHQ). L'interception à partir de fibres optiques serait ainsi délicate en raison de la nécessité pour réaliser une interception de se placer au niveau d'un répétiteur qui amplifie le signal lumineux à intervalles réguliers et du fait que toute intrusion sur la fibre optique est décelée en bout de ligne. Certains experts estiment cependant que les intrusions sont possibles car des dérivations optiques sont réalisables en ayant accès directement aux fibres, par exemple au niveau des centres de distribution, ou en se positionnant sur l'enveloppe des fibres et en captant les ondes extrêmement faibles qui y sont émises ;

— de plus, la multiplication des communications, en dernier lieu sur Internet, rend matériellement impossible l'interception de tous les messages, et *a fortiori* leur stockage et leur traitement.

La possibilité de tri des messages ne réduit pas les difficultés techniques. En effet, les limites des systèmes d'interception sont liées au traitement des données recueillies. Le tri des informations intéressantes à partir des données brutes nécessite les techniques de sélection ou d'extraction les plus perfectionnées. Plusieurs pays disposent de compétences dans ces techniques. Les Russes détiennent certainement des compétences dans le domaine de la sélection. La France dispose de certains atouts dans les technologies des algorithmes et de la linguistique, ce qui favorise les échanges de technologies avec d'autres pays. Mais l'élément le plus important reste la puissance de calcul des ordinateurs. Certaines estimations de spécialistes tendent à montrer que, malgré tous leurs moyens, les services partenaires d'UKUSA ne sont plus en mesure de traiter la masse d'informations recueillies.

Même avec les systèmes de reconnaissance de contexte et de langues, l'un des principaux obstacles viendrait de la langue utilisée. Il paraît de bon sens de comprendre qu'aucune organisation n'est en mesure de traduire des messages pouvant être émis dans les milliers de langues connues. Bien que le système se concentre sur les langues les plus usitées ou liées à des questions de sécurité, on peut se demander si la NSA dispose des locuteurs en nombre suffisant pour l'arabe, le persan, le coréen, le

serbo-croate… L'utilisation d'une langue rare ou disparue renforce la protection du message. L'utilisation d'une langue vivante mais quasi inconnue comme le *navajo* s'est révélée un atout pour les communications des armées américaines dans le Pacifique de 1942 à 1945.

— enfin, le développement des techniques de cryptologie des messages diminue les capacités de traitement et d'analyse, car la puissance de calcul alors requise est impressionnante. Malgré l'ampleur de ses moyens, la NSA n'aurait pas les moyens pour traiter l'ensemble des messages cryptés et les analyser, même si les écoutes ont été ciblées et même si des tris ont été opérés au préalable.

La plupart des interlocuteurs que votre Rapporteur a rencontrés aux Etats-Unis ont fait part de la surestimation des performances du réseau par les médias et ont souligné que les agences fédérales de renseignement, soumises au contrôle étroit du Congrès, notamment sur le plan budgétaire, ne disposaient plus des capacités suffisantes. Certains spécialistes ont même caractérisé la NSA de « dinosaure » dépassé par l'évolution des technologies et la masse d'informations. D'ailleurs, les responsables de la NSA se plaignent de régresser en capacités et les membres du Congrès n'apprécient pas les performances de cette agence.

— en tout état de cause, quelles que soient les performances du réseau Echelon, il doit être complété par d'autres systèmes de renseignement, humain ou technique. En effet, la capacité d'analyse est primordiale, notamment en matière de terrorisme et les services doivent disposer de compétences humaines et d'une culture qui peut leur manquer parfois, notamment aux Etats-Unis.

Pour les membres du Congrès et leurs collaborateurs rencontrés à Washington, comme pour de nombreux spécialistes américains, les enjeux de sécurité supposeraient que les capacités des systèmes d'interception des communications soient renforcées et qu'un nouveau système plus performant remplace le réseau Echelon.

L'ensemble des interlocuteurs s'est finalement prononcé en faveur d'un principe de précaution, au nom des enjeux de sécurité, afin de contrer des capacités dont l'appréciation est impossible.

c. les raisons de la médiatisation actuelle

L'une des principales questions auxquelles votre Rapporteur a cherché à répondre concerne les raisons de l'importance accordée par les médias depuis quelques années au phénomène alors que tout spécialiste

travaillant dans un service de renseignement ou sur les systèmes d'écoute était informé des relations étroites entre les services britannique et américain, connaissait l'existence du réseau Echelon, sinon du pacte qui le sous-tendait, et que les premières informations à son sujet remontent au milieu des années 80. Le journaliste Duncan Campbell a publié, pour la première fois, un article détaillé sur le sujet le 12 août 1988 et n'a pas cessé depuis de rédiger des textes ou de mener des enquêtes d'investigation en ce domaine. De même, le journaliste et écrivain James Banford a publié en 1983 un premier ouvrage sur la NSA évoquant le réseau UKUSA.

De nombreux interlocuteurs de votre Rapporteur ont souligné l'intérêt qu'il y aurait de savoir à qui profite la médiatisation actuelle.

1. Les raisons avancées le plus souvent

a) La critique de la déviation du système

Durant de nombreuses années au cours de la guerre froide, il y a eu un consensus pour ne pas évoquer publiquement le sujet des écoutes. Depuis le début des années 90, ce consensus s'est effrité en raison de la prise de conscience que, si les intérêts militaires pouvaient justifier un système général d'écoutes, il n'en était plus de même pour les écoutes à finalité économique.

Il est certain que de nombreux pays se livrent à des interceptions de communications dans un but économique. Mais un tel objectif est la plupart du temps inavouable.

b) La rupture du lien entre les membres du Pacte

Cette hypothèse repose sur le fait que les changements de gouvernement en Australie et en Nouvelle-Zélande à la fin des années 90 ont amené une modification des attitudes de ces deux pays à l'égard du pacte UKUSA. Il n'est pas sans signification de rappeler que, parmi les premiers à évoquer le réseau Echelon figurent des journalistes ou des hommes politiques de ces deux pays. Ce sont les confidences ou les auditions d'anciens membres des services de renseignement qui ont permis à ces journalistes de mieux comprendre comment fonctionnait le réseau et quelles étaient les cibles des écoutes.

Certes, les tensions entre partenaires sont concevables en raison, non seulement des différences dans les capacités, voire de la disproportion de leurs capacités, mais du fait du rôle de la NSA qui centralise l'ensemble des données collectées et les redistribue, donc les filtre.

Le cas du Royaume-Uni reste cependant à part dans la mesure où seul ce pays dispose des capacités qui lui permettent d'analyser les documents et d'instaurer avec les Etats-Unis des relations « moins inégales » qu'avec les autres membres du pacte.

Mais aucun interlocuteur de votre Rapporteur n'a cru sincèrement à un relâchement des liens entre les partenaires d'Echelon. Tout au plus, une certaine rivalité entre services de renseignement anglo-saxons ne serait pas exclue, certains ne retirant pas le maximum de leur participation au système. M. Nicky Hager estime quant à lui que les liens entre l'agence néo-zélandaise GCSB et la NSA se sont même renforcés depuis les années 80 (éventuellement sans que les autorités politiques aient donné leur accord).

c) L'influence des groupes de pression américains au nom de la défense des libertés individuelles et de la protection des règles du commerce

Les activités des réseaux d'écoute, même motivées par des considérations d'ordre collectif ou de sécurité nationale, sont de nature à porter atteinte aux libertés individuelles.

Les premières enquêtes complètes de journalistes, comme l'australien Nicky Hager ou le britannique Duncan Campbell, correspondent à une évolution de l'opinion publique face aux problèmes que posent les services de renseignement à une démocratie.

Mais les acteurs les plus dynamiques face à Echelon sont sans conteste les groupes de pression américains. Les nombreux sites Internet dédiés à Echelon ou aux services de renseignement de manière générale témoignent de l'efficacité et de la puissance financière de ces lobbies. On peut alors se demander qui soutient financièrement de tels groupes de pression et quels sont fondamentalement leurs objectifs.

Deux phénomènes peuvent expliquer l'intérêt à l'égard d'Echelon :

— la prise de conscience que les libertés publiques étaient directement menacées et que les écoutes portaient préjudice aux citoyens. Cette prise de conscience a débuté aux Etats-Unis sous l'influence d'ONG par exemple de la National Sécurity Archives (Jeffrey Rickelson ?) et a été favorisée par la possibilité ouverte par le *Freedom Act* de demander aux autorités des documents.

L'activisme de certaines organisations soucieuses de bonne conscience est réel et il peut être tentant d'émettre des hypothèses de manipulation compte tenu par exemple des moyens financiers dont elles disposent. Mais aucune preuve n'est apportée de cette manipulation.

— les autorités américaines et australiennes ont donc été contraintes de reconnaître l'existence de réseaux d'écoutes tout en développant une politique de communication visant à préserver le système lui-même sans véritable transparence sur les questions essentielles. La transparence sur des questions mineures sert à dissimuler l'important. L'un des points non avoués consiste par exemple en l'existence d'un second réseau entre membres d'UKUSA sur l'analyse et l'échange de renseignements traités.

Seuls les citoyens américains sont protégés par les lois fédérales sur les écoutes. Pour eux, les règles sont strictes et les écoutes qui les concernent doivent être détruites au bout de 24 heures. Les règles du jeu sont différentes pour les non-américains, auxquels ne s'applique aucune règle particulière. C'est pourquoi les citoyens américains qui se préoccupent de leur protection sur le sol des Etats-Unis et non des écoutes « outre-mer » semblent peu s'intéresser à Echelon, dont ils considèrent généralement qu'il ne les concerne pas.

Pourtant, la NSA recueille des informations sur les citoyens américains. Aux yeux de certains observateurs américains, le vrai danger d'Echelon n'est pas l'espionnage économique mais les atteintes aux libertés publiques (sujet sensible depuis le Watergate). De plus les erreurs sont fréquentes.

On ne cite que deux affaires d'écoutes de sociétés européennes en vingt ans. Ce qui montre soit que la NSA n'est pas très compétente, soit qu'elle ne pratique pas d'écoutes économiques.

A l'inverse, il y a de nombreux cas où les droits des personnes sont violés. Dans le nouvel ouvrage de M. James Banford, des cas de victimes précis seront cités avec des preuves solides. Il ne faut pas oublier que, dans le cadre des écoutes, lorsqu'une information concerne un citoyen d'un des cinq pays de l'accord UKUSA, le nom de ce citoyen n'est pas divulgué, ce qui n'est pas le cas pour les autres. L'analyste peut faire une erreur et indiquer des noms de personnel dans les rapports qui sont diffusés dans le réseau mondial.

d) L'intervention du Parlement européen

Les premières études menées par le Parlement européen ont été, selon de nombreux interlocuteurs, déterminantes pour attirer l'attention de l'opinion publique sur le système Echelon. Votre Rapporteur consacrera à l'intervention du Parlement européen une partie importante de son rapport.

2. Les hypothèses extrêmes

Votre Rapporteur souhaite aborder plusieurs hypothèses qui lui ont été soumises mais qu'il est loin de partager.

Toutes ces hypothèses reposent sur le caractère plausible dans un tel sujet de manipulations de toutes sortes dont la caractéristique commune est qu'elles sont liées à la politique intérieure des Etats-Unis.

a) Les rivalités américaines

Plusieurs idées ont été évoquées à votre Rapporteur. L'une a trait à la rivalité entre agences américaines de renseignement, rivalité accentuée par l'approche des élections présidentielles aux Etats-Unis et par le changement des responsables de ces agences. Une autre hypothèse concerne les négociations entre les agences fédérales, d'une part, le Congrès, d'autre part, les services de renseignement souhaitant un renforcement de leurs moyens d'action, humains comme financiers. L'analyse des débats dans les commissions du Congrès, comme la *House Permanent Select Committee on Intelligence,* révèle une méfiance à l'égard des compétences des agences fédérales NSA ou CIA et la tendance des parlementaires américains à ne pas leur accorder davantage de moyens face aux défis que représentent les progrès technologiques.

b) Une possible mystification

Votre Rapporteur aimerait souligner à l'appui d'une éventuelle manipulation un fait troublant : il a constaté que l'essentiel des documents publiés sur Echelon semblait provenir de la même source. Les renseignements notamment ceux figurant sur Internet sont souvent identiques et donnent l'impression d'avoir été recopiés à partir de deux ou trois sources (les articles et ouvrages déjà cités, les documents déclassifiés de la NSA, etc.). Cette similitude des informations et donc leur relative indigence à l'analyse peuvent témoigner d'une volonté délibérée d'orienter le débat sur les interceptions des communications, volonté à laquelle la communauté du renseignement ne serait pas étrangère.

Une première hypothèse, à la limite du *machiavélisme,* porterait sur la sensibilisation des acteurs économiques, rendus soupçonneux face aux intrusions dans leurs systèmes de communications et d'information, et auxquels il serait alors possible de vendre des systèmes de protection non fiables. Votre Rapporteur reviendra sur cette hypothèse en évoquant les défauts délibérément introduits dans les systèmes et les logiciels produits en grande partie aux Etats-Unis, notamment par la société Microsoft. Au demeurant, cette médiatisation n'est pas négative, puisqu'elle participe à la sensibilisation des acteurs économiques, voire des particuliers.

Une autre hypothèse tendrait à minorer la responsabilité des acteurs américains, d'une part en mettant l'accent sur certains objectifs louables des écoutes (lutte contre les trafics de drogue ou la prolifération), d'autre part en insistant sur les erreurs commises même par des pays alliés notamment en matière de corruption économique, enfin en incluant d'autres pays européens dans le système comme l'Irlande, l'Allemagne, plus récemment le Danemark ou la Suisse qui envisage l'installation sur son territoire de stations de réception, voire en dénonçant l'existence de réseaux mis en œuvre par d'autres pays et en particulier le nôtre.

Une nouvelle interrogation peut donc être formulée, celle de l'entente entre services de renseignement. L'existence de clubs informels en matière de renseignement pose la question fondamentale de l'enjeu de ces clubs et de leurs objectifs. Dans de telles structures, bien des possibilités de manipulation et d'orientation des informations sont concevables.

Il ne faut pas par ailleurs oublier que les réseaux d'écoutes des pays participant à Echelon ont fourni l'Alliance atlantique en renseignement avec les déformations inévitables, comme on a pu en constater en Bosnie ou dans le Golfe, sans qu'il y ait de lien organique entre UKUSA et l'OTAN.

D. Les réponses des pays européens face aux systèmes d'interception des communications

Le débat sur le système Echelon et les réactions des gouvernements des pays occidentaux face à son existence sont d'autant plus complexes que d'autres systèmes d'écoute existent et que des liens se sont noués entre les réseaux existants. Une question intéressante consiste donc à déterminer si d'autres pays que les cinq membres fondateurs ne participent pas au réseau, même à des degrés divers.

1. Les réactions officielles à l'existence d'Echelon

Les Gouvernements des pays européens sont restés longtemps silencieux sur les systèmes d'écoutes et, de manière compréhensible, mesurés dans un souci de ne pas compromettre leurs relations bilatérales avec les Etats-Unis. La plupart de leurs réactions récentes ont été suscitées par les interrogations de leurs parlements nationaux.

a) La position du Gouvernement fédéral allemand

Dans les réponses adressées au Bundestag, le Gouvernement fédéral a indiqué qu'il avait pris connaissance des rapports du Parlement européen mais qu'il ne disposait pas d'informations sur l'état actuel de la coopération entre membres du pacte UKUSA ou sur les risques qu'Echelon pourrait représenter pour la vie privée des citoyens ou la compétitivité de l'économie allemande.

L'analyse des rapports européens, faite par les services du Gouvernement, a été transmise à l'organe parlementaire chargé des activités de renseignement dont les membres sont tenus à la confidentialité. C'est pourquoi il n'a pas été possible à votre Rapporteur de recueillir le contenu de cette expertise gouvernementale.

L'impression ressentie, et confirmée par la visite que votre Rapporteur a effectuée à Berlin en juin dernier, est celle d'un certain scepticisme des responsables politiques quant aux potentialités d'un réseau mondial d'écoutes dont la capacité semble ainsi avoir été « *pour une grande part exagérée* ».

La position du Gouvernement fédéral est cependant empreinte d'ambiguïtés en raison de l'existence de la station américaine de Bad Aibling basée sur le territoire allemand. Les personnes rencontrées par votre Rapporteur lui ont indiqué que les informations recueillies par cette station

étaient communiquées aux services de renseignement allemands. Ils ont précisé que, dans le cadre du débat public qui s'est instauré sur Bad Aibling depuis la chute du mur de Berlin, les Etats-Unis ont donné dès 1998 la garantie qu'ils ne procédaient à aucune écoute qui portait préjudice aux intérêts allemands, l'activité de la station reposant sur le statut des forces OTAN, et qu'ils ne fournissaient pas d'informations aux entreprises américaines. Toute violation de cette garantie entraînerait un incident diplomatique entre les deux pays. Un groupe de députés du Bundestag s'est rendu pour la première fois sur le site en mai 2000 dans le cadre de la commission sur le contrôle parlementaire des services de renseignement. Un conseiller juridique des services américains a expliqué ce que les agences présentes sur le sol allemand faisaient techniquement et ce qu'elles avaient le droit de faire. Cette transparence exceptionnelle aurait rassuré les parlementaires allemands.

Les services de renseignement de l'Allemagne ont désormais accès aux moyens d'écoutes pour évaluer les informations recueillies et utiliser ces moyens en fonction de leurs objectifs et de leurs priorités. Mais, à la question qui a été posée sur le contrôle réellement effectué par les autorités allemandes, il a été répondu que celui-ci n'était pas mis en œuvre puisque les relations germano-américaines reposaient sur la confiance.

Cependant, selon les mêmes interlocuteurs, la coopération nécessaire entre services de renseignement ne doit pas être « *polluée* » par des atteintes dans les domaines économiques. Selon eux, cette position n'implique pas que toutes les conjectures relatives au rôle d'Echelon soient dépourvues de fondement, mais elle répond au souci qu'aucune action illicite ne se produise, la nécessaire coopération face aux nouvelles menaces ne devant pas être entachée par la méfiance de l'espionnage économique. Ces responsables évoquent donc le climat de « *confiance vigilante* » qui doit s'instaurer entre Alliés et prônent la réduction de cette méfiance par des échanges d'informations et l'élaboration d'un code de conduite pour régler les éventuels incidents.

b) La position des autorités belges

Le Parlement belge a organisé un contrôle indirect des services de renseignement belges. La loi du 18 juillet 1991 a institué deux comités permanents de contrôle des services de police et de renseignement (comités P et R) formés d'experts et sous le contrôle de deux commissions parlementaires spéciales. Ces commissions ont saisi le comité R en juillet 1998 afin qu'il mène une enquête sur la réaction des services belges de renseignement *« face à l'éventualité d'un système Echelon d'interception des communications en Belgique »*. Le comité R a rendu successivement

deux rapports, l'un en août 1999, l'autre en juillet 2000, le second incorporant l'expertise de deux universitaires « indépendants ».

Le premier rapport a établi que les services belges de la Sûreté de l'Etat et du Service général du Renseignement (SGR) avaient uniquement connaissance du système Echelon par l'intermédiaire des sources ouvertes d'information et que, faute de moyens, ils ne menaient pas d'enquête particulière. Les auditions de responsables des services belges de renseignement au printemps 2000 ont confirmé, soit un certain désintérêt de ces services (la protection du potentiel économique et scientifique n'entrant pas dans les missions des services officiels), soit un fatalisme des autorités (absence de compétences techniques ou légales).

Les deux experts mandatés par le comité R ont rendu le 7 mars 2000 un rapport sur le réseau Echelon qui analyse les sources ouvertes, prend position sur la vraisemblance des hypothèses avancées par le STOA, décrit les technologies utilisées et l'environnement juridique des interceptions des télécommunications. Ses conclusions sont assez « maximalistes » dans la mesure où elles reconnaissent une grande capacité technique au réseau Echelon et insistent sur la nécessaire sécurité des communications dans un contexte démocratique. Devant les incertitudes relatives aux activités des services alliés de renseignement, les deux experts préconisent l'agrément des appareils au niveau européen et la création d'une structure centrale de sécurité des systèmes d'information.

C'est pourquoi le comité R a préconisé, non seulement la création d'un organe interministériel de concertation, mais également une politique de sensibilisation des entreprises et des universités aux menaces d'interception de leurs communications.

Par ailleurs, au nom du principe de précaution, les services officiels recommandent de prendre des initiatives en matière de sécurité informatique et souhaitent que soit définie une politique nationale du chiffrement. La loi du 19 décembre 1997 a libéralisé l'usage de la cryptographie en Belgique à un niveau de 128 bits pour les systèmes de clés.

c) La position des autorités britanniques

L'existence d'une base d'écoutes des communications à Menwith Hill a été reconnue à plusieurs reprises par les Ministres successifs de la Défense en réponse à des questions parlementaires. Il a même été précisé qu'y travaillaient près de 1 200 employés américains et 600 britanniques (ce qui témoignait non seulement de la participation du Royaume-Uni au système Echelon mais de l'imbrication de ses services de renseignement avec les agences fédérales et l'US Air Force), que la base comportait 21 radômes sur 125 hectares et qu'aucune activité contraire aux intérêts britanniques n'y était autorisée, la présence des personnels du Royaume-Uni apportant une garantie.

Si aucune société n'a déposé de plainte, des procédures judiciaires ont cependant eu lieu et vont avoir lieu. Ainsi, la suite de la procédure judiciaire engagée début juillet par le Procureur de la République de Paris, les autorités britanniques ont affirmé qu'elles étaient disposées à collaborer avec les autorités françaises et ont réaffirmé que les stations britanniques n'étaient pas utilisées à des fins d'espionnage économique.

Mais la position du Royaume-Uni est ambiguë comme en témoignent deux événements. Le premier a trait au procès fait à deux personnes ayant tenté de pénétrer sur une base et au témoignage d'un responsable de British Telecom. Le juge britannique a alors conclu que les impératifs de défense nationale exigeaient que l'affaire reste secrète. L'autre événement concerne la démission d'une employée du GCHQ, Mme Margareth Newsham, qui a fait des révélations sur le système Echelon comme le rapporte Duncan Campbell.

d) La position du Gouvernement français

Notre pays est certainement l'un des plus sensibles à Echelon car des initiatives américaines peuvent avoir eu comme effet de contrer non seulement la politique de dissuasion nucléaire mais aussi la politique d'exportation de la France dans des zones géographiques considérées comme réservées, même s'il s'agit vraisemblablement d'initiatives pragmatiques et non d'une stratégie politique délibérée.

Les interrogations des parlementaires français sur Echelon sont récentes. Plusieurs types de réponses ont été fournis par le Gouvernement :

— le Garde des Sceaux, Mme Elisabeth Guigou, a admis dans une séance de questions au Gouvernement, que le réseau Echelon était « *détourné à des fins d'espionnage économique et de veille concurrentielle* » ;

— le Ministre de l'Intérieur, M. Jean-Pierre Chevènement, a quant à lui estimé qu'un tel détournement appelait « *une particulière vigilance* » et il a recommandé « *la prudence et la discrétion des utilisateurs* » ;

— le ministère des Affaires étrangères, très sensible à la mise en cause des libertés individuelles et de la confidentialité des communications, a été très en pointe pour la libéralisation des procédures de cryptage lors des réflexions interministérielles car elle lui paraissent de nature à protéger les intérêts français. C'est pourquoi il s'est montré favorable à la mise en place d'un mécanisme de veille technologique ;

— au contraire, le Ministre de la Défense, M. Alain Richard, qui assure la tutelle de trois services de renseignement (la DGSE, la DRM et la DPSD), a tenu un discours moins explicite, évoquant « l'objectif de sécurité nationale ».

La position du Gouvernement français pourrait être amenée à évoluer pour deux raisons :

— la poursuite du travail d'investigation de diverses instances parlementaires amènera le Gouvernement à préciser sa politique en matière d'écoutes et de lutte contre les intrusions ;

— l'engagement de procédures judiciaires conduit à des enquêtes. Pour la première fois, une association de défense des utilisateurs d'Internet (Akawa) a porté plainte en mars dernier contre X pour violation du secret des correspondances devant le Tribunal de grande instance de Paris. De même, à la suite du dépôt de plaintes du député européen Thierry Jean-Pierre, le procureur de la République de Paris, M. Jean-Claude Dintilhac, a ouvert une enquête préliminaire qui a été confiée à la DST, le 24 mai dernier.

2. Les réticences des services de renseignement

Trois raisons peuvent expliquer la position réticente des services de renseignement face au système Echelon :

— les liens de coopération entre les services de renseignements ;

— l'internationalisation des services de renseignement qui comporte plusieurs volets dont des contacts entre services et des liens plus ou moins informels ;

— l'existence d'écoutes réalisées par les services nationaux de certains Etats, même si celles-ci n'ont ni la vocation ni l'ampleur du système Echelon.

a) La tradition de coopération bilatérale entre services de renseignement

Si la collaboration avec le système Echelon ne fait aucun doute pour le Royaume-Uni compte tenu de son rôle dans le pacte UKUSA, la position d'autres membres de l'Union européenne n'est pas toujours dénuée d'ambiguïtés en raison notamment d'échanges d'informations, voire de la participation, directe ou indirecte, de leurs services de renseignement aux activités du réseau.

L'historique et le développement des réseaux d'interception des communications illustrent l'action commune des Alliés face au Pacte de Varsovie. Après 1966, le renseignement est l'un des trois domaines de l'organisation militaire intégrée de l'OTAN que la France n'a pas réellement quittés. La France disposait de son propre réseau d'écoutes, un créneau d'écoutes des armées ennemies lui était confié et des échanges officiels et réguliers étaient organisés. Même si un tel créneau d'écoutes n'existe plus, les échanges s'effectuent toujours. Ils sont plus que jamais nécessaires dans la mesure où les services de renseignement ont besoin d'élargir leurs bases de données pour accroître leurs performances et déchiffrer les messages cryptés, même *a posteriori.*

Les échanges existent entre services au niveau des productions brutes (les écoutes), des savoir-faire et des compétences. En fait, on distingue deux catégories d'échanges :

— au niveau technique, les échanges sont assez développés. Les données recueillies donnent lieu à un véritable marchandage entre les

services de renseignement dans des bourses d'échanges « totems » ou au sein de clubs (comme celui dit « de Berne »). Les technologies permettant des écoutes « croisées », Echelon est d'abord un accord d'échanges de données brutes entre plusieurs pays ;

— au niveau du renseignement plus élaboré, les échanges sont plus difficiles car les services sont réticents et très prudents pour valider leurs éléments. Dans le domaine du renseignement d'intérêt militaire et dans le cadre d'une alliance, les moyens fonctionnent avec la participation de tous les alliés qui contribuent ainsi au renseignement de théâtre du commandant militaire de l'opération.

Pour accroître leurs performances, les services doivent développer leur collaboration avec les alliés, même dans les sujets les plus sensibles. C'était aussi l'intérêt de la NSA d'avoir des contacts avec les services français. La France a su maintenir ces contacts et ces échanges en gardant une certaine indépendance.

Selon certains interlocuteurs de votre Rapporteur, des personnels français auraient été formés aux Etats-Unis. La France aurait ainsi bénéficié des savoir-faire acquis par les responsables d'Echelon. Il est vraisemblable aussi que l'architecture du réseau français d'écoutes a été inspirée de celle de ses alliés britannique et américain (le réseau a été développé en faveur de l'Alliance atlantique, dont la France est membre). Certains des interlocuteurs ont même indiqué que notre pays ne disposerait pas actuellement de capacités techniques aussi développées si les Etats-Unis ne l'avaient pas aidé. La notion de transfert de technologies est sans doute trop forte pour qualifier les relations entre la France et les Etats-Unis mais des aides ou des échanges sont certains. Certains services reconnaissent d'ailleurs des liens qu'ils ne qualifient pas « d'ordre majeur ».

Même après le départ de la France de la structure militaire intégrée de l'OTAN, il y avait une alliance objective d'intérêts. M. Henry Serres, directeur du DCSSI, a été le fondateur de la direction technique de la DGSE.

Les Etats-Unis ont organisé des rencontres annuelles avec la plupart des pays européens. Fondées par le FBI en 1993, ces rencontres sont dénommées ILETS (*International law enforcement Telecommunications Seminars*).

b) Les systèmes nationaux ou multinationaux

Certains pays ont développé des réseaux d'interception des communications, mais sans aucune comparaison avec Echelon, dont ils n'ont ni l'ampleur ni la vocation. Ces systèmes restent à finalité opérationnelle militaire. Comme il est impensable d'afficher des objectifs économiques pour la création d'un réseau européen et que la sécurité au sens militaire n'en fait pas une nécessité, on voit difficilement comment pourrait prendre forme une coopération européenne.

La France dispose de réelles capacités d'écoute dont certaines sont enviées et ont fait preuve de leur intérêt lors des conflits récents (écoutes HF par exemple pendant la Guerre du Golfe ou en Bosnie). Les services français ne disposent pas de moyens suffisants pour avoir une panoplie complète de dispositifs d'écoute même si la baisse des budgets d'équipement de la défense a relativement épargné ces services dont la part augmente donc en pourcentage tout en restant faible en valeur absolue. De plus, les moyens actuels sont terriblement sollicités face à l'émergence de menaces que l'on ne contrôle pas. Ils ne sont plus disponibles pour la formation aux techniques modernes. Ils sont géographiquement orientés et limités et ne peuvent en aucune façon être comparés au réseau Echelon. On ne saurait donc parler de « *Frenchelon* ».

De manière générale, la tradition du secret est néfaste pour les services de renseignement eux-mêmes car elle peut mettre leur existence en péril. Pour les journalistes, les errements des services sont souvent liés à des considérations politiques.

Le Gouvernement parait encore défavorable à la mise en place d'une structure de contrôle parlementaire. Mais les officiers de renseignement de terrain avec lesquels des contacts restent possibles sont favorables à un contrôle des objectifs et des moyens des services de renseignement.

Un tel contrôle parlementaire devra, de toute manière, être de nature globale et vérifier l'adéquation entre les moyens accordés aux services et les missions qui leur ont été fixées.

conclusion de la première partie :

Vers une stratégie globale

de contrôle de l'information ?

Au terme de ses recherches, votre Rapporteur a acquis les certitudes suivantes :

— il existe effectivement un système d'interception des communications, mis en œuvre par les services de renseignement des Etats-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande. Ce système s'est développé de manière spectaculaire dans les années 70 et 80, et la fin de la guerre froide, qui avait justifié sa création, n'a pas entraîné sa disparition. Son existence est attestée par le fonctionnement de bases ou de stations d'écoutes dans les cinq pays membres du pacte et d'autres Etats comme le Japon ou l'Allemagne, par de nombreux témoignages et par certains documents déclassifiés ou rendus publics accidentellement ;

— si les enjeux de sécurité au sens large justifient pour ses créateurs le maintien d'un tel système, il n'est pas impossible que certaines informations recueillies puissent être utilisées à des fins politiques et économiques. Il n'existe pas de preuve formelle de détournement du système, mais l'ambiguïté des déclarations de certains responsables ne laisse aucun doute sur cette possibilité ;

— même si aucune entreprise française ne s'est plainte d'écoutes, les *aveux* non démentis d'anciens responsables de services américains, au-delà de leur aspect provoquant et moralisateur, tendent à prouver que, dans les affaires citées par les médias et touchant des entreprises européennes, des interceptions ont bien bénéficié indirectement à des sociétés américaines. Si les autorités françaises conseillent aux entreprises et aux acteurs économiques de se protéger, elles ont nécessairement leurs raisons ;

— la question de la protection des libertés publiques est indissociable de l'analyse des capacités réelles des réseaux d'interception des communications et de l'interprétation que les services nationaux de renseignement font de la réglementation des écoutes dans les différents pays. Plus les systèmes sont vulnérables, plus ils sont écoutés. Même les réseaux filaires ne sont pas épargnés mais, dans ce cas, un doute subsiste sur la possibilité d'intercepter les communications à une échelle mondiale ;

— les moyens acquis depuis quarante ans par les services de renseignement acteurs d'Echelon permettent de recueillir, sinon de traiter, un grand nombre de communications. Cependant, l'explosion des communications et le développement des mesures protectrices, en particulier le chiffrement des messages, compliquent la tâche de ces services pour l'exploitation des données recueillies et ceux-ci sont sans doute dépassés sur certains créneaux. Une des principales limites des réseaux d'écoutes proviendrait de leur prochaine obsolescence au niveau des technologies ;

— le débat s'est en fait déplacé de l'intrusion sur les réseaux de communications à l'intrusion dans les réseaux informatiques, c'est-à-dire au plus près de la source émettrice du message.

Votre Rapporteur est ainsi convaincu de la vulnérabilité des systèmes d'information et de communication (SIC) face aux écoutes et aux intrusions directes qui ne pourront que croître. La question fondamentale n'est donc plus celle de l'illégalité des écoutes ni de leur détournement, même si les problèmes de fond ne sont pas pour autant réglés (prédominance de certains Etats qui utilisent un système à leur profit, atteintes graves aux droits fondamentaux des individus, voire au fonctionnement régulier des institutions).

Avoir une vision prospective nécessite de renforcer la protection des SIC à tous les niveaux, individuel et collectif, national et européen.

II. — Les moyens de protection des systèmes de communications

A partir du moment où la confidentialité des communications est devenue imparfaite, il est de la responsabilité des opérateurs de se protéger et de déterminer ce qui doit être protégé compte tenu des enjeux politiques ou économiques. De nombreux moyens existent pour se protéger des intrusions dans les systèmes de communications et renforcer leur sécurité. De nombreuses méthodes traditionnelles méritent d'être évoquées comme le contrôle des accès, le cloisonnement ou l'isolement des réseaux, l'installation de barrières (« *firewalls* ») ou le filtrage des paquets d'information transmis par exemple sur Internet.

Certaines méthodes font appel à la *stéganographie,* c'est-à-dire que le message confidentiel est caché dans un ensemble anodin. On a ainsi cité à votre Rapporteur l'exemple de supports comme la modification des pixels d'une photographie qui recèle en elle-même un contenu informatif.

Mais le procédé le plus couramment utilisé et qui complète les méthodes traditionnelles de confidentialité et de sécurité relève de la *cryptologie*. La cryptologie, science de l'écriture secrète, englobe la cryptographie qui est la technique du chiffrement des messages, et la cryptanalyse qui est la recherche du texte en clair sans connaissance du chiffre.

Les deux schémas suivants illustrent les principes de base de la cryptographie. Toute l'histoire des codes secrets montre que le chiffrement s'effectue selon les principes de substitution et de transposition des éléments (en général les lettres), et que les progrès de la cryptographie ont été menés en parallèle avec ceux de la cryptanalyse.

A. La cryptologie

1. L’historique de la cryptographie : une dynamique sans cesse en évolution

Trois étapes majeures ont été réalisées dans l'histoire des mécanismes de chiffrement :

— l'invention du chiffre monoalphabétique dès l'Antiquité ;

— la mécanisation des opérations de chiffrement et de déchiffrement puis le recours aux ordinateurs ;

— la création du système de clés dites publiques.

a) L'utilisation de chiffres alphabétiques

En raison de sa simplicité et de la multiplicité des combinaisons, le principe de substitution a dominé les techniques de cryptographie pendant le premier millénaire de notre ère. Mais le cryptage avec un seul alphabet comme le chiffre décalé de Jules César n'a pas résisté aux expériences des cryptanalystes arabes qui, se fondant sur la linguistique et les statistiques, réussirent à déchiffrer des messages sans en connaître la clé. Ils se basèrent sur l'analyse des fréquences d'apparition des lettres dans une langue donnée.

Le développement des relations diplomatiques au Moyen-Age et à la Renaissance favorisa l'explosion des procédés de cryptographie. L'utilisation des mots code fut abandonnée en raison de ses limites, notamment de la nécessité de disposer de dictionnaires et de modifier souvent les codes. Par contre, l'utilisation simultanée de plusieurs alphabets pour crypter un message trouva son apogée dans le carré de Vigenère.

On utilisa aussi des chiffres de substitution qui remplaçaient les lettres par des substituts, le nombre de ces substituts restant proportionnel à la fréquence de la lettre ou d'un groupe de lettres (exemple du grand chiffre de Louis XIV).

Ces différentes méthodes n'ont cependant pas résisté aux cryptanalystes qui se sont fondés sur l'analyse des répétitions et des caractéristiques de la langue employée (relations des lettres entre elles). C'est ainsi que l'anglais Charles Babbage proposa une méthode pour briser le chiffre de Vigenère au milieu du XIX^{ème} siècle.

La faiblesse des cryptages reposant sur la clé de chiffrement et de déchiffrement, plusieurs améliorations furent apportées en particulier l'utilisation des clés aléatoires qui sembla la plus prometteuse mais buta sur la nécessité de distribuer l'ensemble de ces clés aléatoires aux opérateurs.

b) De la mécanisation à l'utilisation des ordinateurs

Les cryptanalystes permirent de briser les codes allemands pendant la première guerre mondiale comme le montre l'exemple du télégramme du Ministre allemand des Affaires étrangères Arthur Zimmermann qui cherchait à faire entrer le Mexique dans une guerre avec les Etats-Unis et qui servit aux Britanniques à persuader le président Wilson d'intervenir dans le conflit.

C'est pourquoi la mécanisation du chiffrement fut entreprise entre les deux guerres par des allemands, en particulier Arthur Scherbius qui mit au point la machine mécanique *Enigma*. Celle-ci équipa les armées allemandes pendant la seconde guerre mondiale. Les efforts des Polonais puis des Britanniques (dans le fameux centre de Bletchley Park) permirent de trouver des parades et de déchiffrer les codes allemands grâce à la mise au point de machines dédiées et dotées d'électronique, les « bombes », véritables ancêtres des ordinateurs.

L'un des progrès les plus importants apportés à la cryptographie fut donc l'utilisation des premiers ordinateurs qui alliaient complexité et rapidité, et travaillaient sur des nombres binaires formés de 1 et de 0 (ce sont les *binary digits* ou bits). La conversion des lettres en chiffres s'effectue alors par exemple au moyen d'un protocole comme ASCII (*american standard code for information interchange*).

A mesure que les ordinateurs se sont répandus, la cryptographie est devenue accessible aux entreprises voire aux particuliers, et n'est plus restée l'apanage des autorités publiques. C'est pourquoi le *National Bureau of standards* aux Etats-Unis a demandé que soit créé un système standard de chiffrement. La NSA a plaidé pour la limitation du nombre de clés utilisées dans le chiffrement à 10^{17} (soit une clé de chiffrement à 56 bits puisque 10^{17} s'écrit en 56 chiffres binaires).

Le chiffre *Lucifer* de Thomas Feistel a été officiellement adopté le 23 novembre 1976 : le *Data Encryption Standard* (DES), développé par IBM, est longtemps demeuré la norme officielle de chiffrement. Face à son obsolescence, la génération suivante de standard de chiffrement, nommée AES (*Advanced Encryption Standard*) a fait l'objet d'un appel d'offres international qui vient d'être remporter par un système de cryptage belge *Rijndael*.

c) La cryptographie à clés publiques

Le problème primordial du chiffrement a toujours été celui de la

distribution des clés entre envoyeurs et receveurs car cette transmission fragilise le dispositif entier du chiffrement et devient impossible à gérer face au développement des communications.

La clé est le paramètre qui transforme le système général de chiffrement en le spécifiant pour ses utilisateurs. Elle ne doit être connue que de l'émetteur et du receveur. On a longtemps utilisé des mots-clés. Les systèmes traditionnels de chiffrement ont toujours été symétriques ce qui signifie que le procédé de déchiffrement est l'inverse du procédé de chiffrement et que le secret unique, la clé, est détenue par les intervenants autorisés.

Une première étape a été franchie par la découverte par trois chercheurs américains (Whitfield Diffie, Martin Hellman et Ralph Merkle) au milieu des années 70 de la possibilité d'échanger des informations cryptées sans avoir besoin de se rencontrer au préalable pour échanger une clé secrète. Pour cela ils imaginèrent de crypter les messages avec des fonctions mathématiques difficilement réversibles c'est-à-dire que le receveur a besoin de connaître certains éléments pour déchiffrer, ces éléments mathématiques pouvant lui être transmis en clair. En d'autres termes, les messages sont chiffrés par une fonction dite à sens unique et seul le receveur dispose des outils pour inverser cette fonction.

Une seconde étape a consisté à utiliser des clés dites asymétriques par opposition aux procédés traditionnels dits symétriques. Dans un chiffrement asymétrique, les clés de chiffrement et de déchiffrement diffèrent. Le receveur garde secrète une clé de déchiffrement qui s'appelle donc ***clé privée***. Par contre, il peut diffuser sa clé de chiffrement de façon que tous la connaissent ce qui en fait une ***clé publique***. L'ensemble des clés publiques peut figurer dans un annuaire consultable par tous les utilisateurs potentiels. Si quelqu'un veut envoyer un message au receveur, il utilise la clé publique de chiffrement du message du receveur. Seul le receveur pourra décrypter le message grâce à sa clé privée de déchiffrement.

La découverte d'une fonction mathématique adéquate revient à deux équipes de chercheurs, l'une du GCHQ britannique (James Ellis, Clifford Cocks et Malcom Williamson), dont les travaux ont été gardés secrets pendant trente ans, et une autre de trois universitaires du MIT (Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman) qui ont donné leur nom au cryptosystème à clé publique **RSA** inventé en 1977.

Le principe de ce système mérite d'être décrit. L'utilisateur crée sa propre clé en choisissant deux nombres premiers (c'est la clé privée). Une combinaison simple de ces deux nombres premiers est rendue publique

(c'est la clé publique). Seul l'utilisateur connaît les nombres qui ont servi à l'élaborer et qui permettront d'inverser la fonction utilisée pour le chiffrement. Il est pratiquement impossible de déduire les nombres premiers à partir de leur combinaison car les efforts de factorisation pour y parvenir requièrent des moyens informatiques trop importants. Plus les nombres premiers comportent de chiffres, plus la confidentialité est assurée d'où l'importance de la recherche sur les nombres premiers (pour la cryptographie) et sur la factorisation des nombres premiers (pour la cryptanalyse).

Les systèmes mixtes combinent les avantages de la clé secrète et de la clé publique. La clé publique est alors utilisée pour la signature et la distribution des clés secrètes. La clé secrète est chiffrée par la clé publiée et décryptée par le receveur au moyen de la clé privée.

2. Le dilemme de la cryptographie : entre libertés publiques et sécurité nationale

Le dilemme essentiel de la cryptographie tient à l'impossibilité de concilier les exigences des libertés publiques individuelles (protéger la confidentialité des communications privées dans un monde où les échanges sont libéralisés, donc disposer de chiffres impossibles à briser) et les impératifs de la sécurité collective (traquer les messages criminels donc être capable de briser des chiffres ou d'avoir accès à certaines informations cryptées).

a) Les logiciels de chiffrement

Dans l'état actuel des connaissances techniques, notamment mathématiques, il est possible d'estimer à partir de quel degré un chiffre peut être qualifié de robuste ou combien de temps est nécessaire pour le briser.

Une bonne connaissance de l'état des technologies est donnée par la réglementation et les limites que les gouvernements ont fixées. Ainsi, dès les années 70, le gouvernement américain a fixé à 56 bits la longueur maximale des algorithmes standards pour les clés utilisables aux Etats-Unis, les exportations de logiciels ayant été limitées à ceux dont la longueur ne permet pas un chiffrement très sûr. Cette limite permet de penser que la NSA était capable de briser à l'époque les chiffres d'une capacité inférieure ou égale à 56 bits dans un temps raisonnable. Les progrès sont tels que cette capacité doit atteindre aujourd'hui les chiffres à 80 ou 100 bits. Une telle opération est facilitée par le fait que le message crypté contient une information connue en clair, ce qui permet des comparaisons et par l'obtention d'un grand nombre de couples message en clair / message chiffré ; ce qui explique le souci des services de renseignement de disposer d'un maximum d'écoutes.

Un chiffre à 128 bits, comme ceux qui seront dorénavant autorisés en France ou en Belgique, est considéré par certains comme ne pouvant pas être brisé ou du moins d'un niveau suffisant pour les transactions civiles à gros débit ou les communications militaires non confidentielles. La cryptologie fournit alors un excellent moyen de sécurité puisque la durée nécessaire au déchiffrement est suffisamment longue pour que l'information recherchée perde de sa valeur avec le temps. Certains experts pensent qu'un niveau supérieur reste nécessaire pour les communications militaires au moins pour la transmission des clés secrètes. Un chiffre pur à 128 bits est déjà une catastrophe pour les services de renseignement mais il peut être brisé par une recherche mathématique systématique. D'où la nécessité d'aller au moins jusqu'à 1 024 bits pour la transmission des clés privées asymétriques.

La mise sur Internet de logiciels libres de chiffrement (*Pretty Good Privacy* PGP) par l'américain Phil Zimmermann au début des années 90 a heurté de front la NSA qui ne voulait pas que les communications des particuliers puissent être cryptées par des chiffres qu'elle ne pourrait pas attaquer. Phil Zimmermann suggéra d'échanger des messages cryptés avec des chiffres symétriques comme l'IDEA qui permettent des opérations rapides et d'utiliser seulement le système de clés publiques beaucoup plus

lent pour la transmission de la clé de déchiffrement. L'émetteur crypte la clé de déchiffrement avec la clé publique du receveur. Le receveur utilise sa clé privée pour décrypter la clé de déchiffrement et utilise ensuite le système IDEA pour décrypter le message. Il y a donc superposition des deux systèmes.

Les attaques qui ont été menées par la NSA sur le plan judiciaire contre les logiciels *Pretty Good Privacy* ont cessé et la dernière version proposée a reçu l'aval des autorités américaines. Il est donc à craindre que ces logiciels ne soient plus aussi libres que par le passé et que des accords aient été conclus entre les agences fédérales américaines et le concepteur du système.

b) Les systèmes de séquestres et d'authentification

Plusieurs systèmes ont été mis au point ces dernières années pour répondre aux conséquences de la généralisation des clés publiques et de leur nécessaire gestion :

— ***les signatures électroniques.*** Les logiciels PGP facilitent la signature numérique des messages électroniques. L'idée pour un émetteur est d'utiliser sa clé privée pour crypter sa signature et authentifier ainsi le message. Tous les receveurs sont alors capables d'identifier l'émetteur en utilisant sa clé publique pour s'assurer de son identité ;

— par ailleurs, le problème de savoir si un émetteur utilise la bonne clé publique de son correspondant peut se résoudre par l'intermédiaire d'une ***autorité d'authentification*** qui certifie que telle clé appartient bien à telle personne et qu'il n'y a donc pas erreur dans leur utilisation ;

— la question de l'accès aux clés secrètes par les autorités a été résolue par l'instauration des ***séquestres de clés***. En termes de cryptographie, « séquestre » signifie que les émetteurs remettent une copie de leurs clés privées à un tiers agréé qui sera en mesure de transmettre la clé sur demande des autorités de police ou de justice. De même, des ***tiers de confiance*** (*trusted third parties*) peuvent conserver un double des clés privées en cas de perte ou d'oubli par l'utilisateur.

La majorité des personnes rencontrées par votre Rapporteur :

— déconseillent de confier la gestion des clés privées à un organisme centralisé afin d'éviter la création d'une structure ingérable et de multiplier les inconvénients liés au manque de confiance (surtout s'il s'agit d'un organisme public) ou au risque de confidentialité. La gestion serait

donc assurée par les entreprises de manière locale et déconcentrée ;

— renforcer les aspects juridiques en légalisant l'obligation de remise en clair des messages chiffrés.

Les autorités américaines auraient souhaité que les agences gouvernementales jouent le rôle de séquestres. Mais les différents groupes ou associations soucieux des libertés publiques ont refusé car ces systèmes doivent reposer sur la confiance. Or c'est là leur point faible essentiel. En effet, à mesure qu'ils se développent, les systèmes de cryptographie, qui par ailleurs ne sont pas exempts de faiblesses, peuvent être victimes de malveillances ou de pièges : virus infectant les logiciels, versions truquées des logiciels de chiffrement, apparemment anodines mais qui permettent en fait aux concepteurs de logiciels de connaître les messages émis sans avoir même à les décrypter (principe du cheval de Troie).

B. La situation juridique des interceptions et de la cryptologie

Une des questions essentielles relatives au développement de la cryptologie a trait au régime juridique des interceptions des communications et des moyens de les contrer.

Parce que les normes internationales en la matière ne déterminent pas de régime précis et normatif, la base juridique des interceptions ressortit des droits internes de chaque pays.

1. La réglementation internationale concernant les interceptions des communications

a) Un régime international somme toute permissif

Si une protection semble exister contre les interceptions considérées comme illégales en droit national, aucun régime international n'interdit de fait celles autorisées par les Etats.

La raison fondamentale est que deux impératifs contradictoires doivent être conciliés : le respect de la vie privée des individus, donc du secret de leurs correspondances, et les impératifs d'ordre public et de sécurité nationale. C'est pourquoi certaines atteintes à l'encontre des droits individuels ont été tolérées dans la mesure où des objectifs clairs étaient affichés pour les interceptions des communications et où des mécanismes de contrôle étaient institués.

Les Etats-Unis conçoivent une protection limitée de la

confidentialité des communications en raison des intérêts en jeu, qu'il s'agisse du domaine économique ou de la lutte contre les nouvelles menaces. C'est ainsi qu'ils engagent leurs partenaires à un effort international pour augmenter les capacités légales d'interceptions et qu'ils souhaitent que les Etats membres de l'Union européenne incorporent le même type de dispositions et suivent des procédures identiques. Le Congrès a adopté, en 1994, la loi *Calea* qui oblige les fabricants de matériels de télécommunications à faciliter les interceptions légales des communications à la demande des organismes officiels.

b) L'absence de réglementation européenne

Il n'y a pas de réglementation européenne des écoutes et des interceptions de communications privées. Les seuls textes existants n'ont pas de caractère contraignant et reflètent seulement une orientation politique.

La Convention européenne des Droits de l'Homme, signée à Rome le 4 novembre 1950 mais ratifiée définitivement en 1997, garantit en effet en son article 8 le respect de la vie privée et familiale du domicile et de la correspondance. Comme la convention signée à Strasbourg le 28 janvier 1981, elle ne contient pas de règles directement applicables dans l'ordre juridique interne des Etats membres mais énonce des principes que les Etats s'engagent à respecter en accordant leur législation à ces principes. Plusieurs arrêts notamment *Klass v. Germany* (1978) ou *Leander v. United Kingdom* (1987) ont précisé les conditions de l'immixtion possible d'un Etat en matière d'interception des communications. Est-il utile de préciser qu'un réseau comme Echelon ne remplit aucune de ces conditions ne serait-ce que parce que les interceptions sont réalisées sur la base de la recherche systématique et que la collecte de données n'est pas limitée par les stricts besoins de sûreté de l'Etat ?

Par ailleurs, la jurisprudence développée par la Cour européenne des droits de l'homme sur la base de la Convention européenne des droits de l'homme a eu des répercussions sur les règles nationales en matière d'écoutes judiciaires ou administratives dont les systèmes sont cependant sans commune mesure avec les réseaux d'interception globale.

La protection des données à caractère personnel fait cependant l'objet d'une réglementation européenne plus précise dont deux directives récentes de l'Union européenne :

— celle adoptée le 25 octobre 1995 par le Parlement européen et le Conseil (n° 95/46/CE) est 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 sur une proposition de la Commission, 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 télécommunication dans la Communauté, et suite à l'avis du Comité économique et social du 3 avril 1991.

Cette 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* ». De même, l'article 29 institue un 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, adopté le 25 juin 1997, couvre la situation observée en 1996 dans ce domaine. Le deuxième rapport, en date du 30 novembre 1998, met en avant les évolutions enregistrées en la matière ;

— le Parlement européen et le Conseil ont arrêté, le 15 décembre 1997, la directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (suite à la position commune adoptée par le Conseil des Ministres le 12 septembre 1996). Cette seconde 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 télécommunication à l'égard du traitement des données.

Elle précise, pour le secteur des télécommunications, les règles générales énoncées dans la directive 95/46/CE et renforce la protection de la vie privée et des intérêts légitimes des abonnés. Mais son champ d'action est plus étendu, car 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 en effet 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 »*. Son article 5 précise ainsi que :

« Les Etats 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 les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées. ».

c) Le cas particulier des interceptions légales

En ce qui concerne les interceptions légales des communications, seules deux résolutions du Conseil marquent un début d'engagement politique. La première, en date du 17 janvier 1995, semble marquée par l'influence des Etats-Unis, car elle reprend les souhaits invoqués par l'administration américaine, notamment le souci de disposer de normes comparables pour simplifier les interceptions sur le plan technique. Le second projet, adopté le 3 décembre 1998, prenait en compte l'évolution des technologies et visait à modifier la première résolution. 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.

Alors que l'avis de la Commission juridique des droits des citoyens, adopté le 25 mars 1999, rejette la proposition du Conseil jugée imparfaite, imprécise et de nature à porter préjudice aux droits des individus, le rapport que la Commission des libertés publiques et des affaires intérieures a rendu le 23 avril 1999 approuve la proposition du Conseil à quelques réserves près et propose que le Parlement soit à nouveau consulté au cas où le Conseil apporterait des modifications substantielles. Ainsi, en adoptant le rapport, le 7 mai 1999, par le vote d'une résolution législative, le Parlement a approuvé le projet de résolution du Conseil, tout en rappelant l'impérieuse nécessité de respecter la protection des données à caractère personnel. Il demande donc au Conseil de vérifier avant le 1er juillet 2000 dans quelle mesure les Etats membres ont transposé cette résolution ainsi que celle de 1995.

2. Le renvoi aux dispositifs nationaux

a) Le cas des pays européens

Les différents Etats membres de l'Union européenne disposent chacun d'une réglementation sur les interceptions des communications. Les principes généraux sont souvent similaires dans la mesure où les directives

européennes sur la protection des données à caractère personnel ont été transposées en droit interne. Mais le cadre juridique des moyens faisant appel à la cryptologie diffère encore selon les Etats et toutes les situations se rencontrent, de l'absence de règles contraignantes permettant un régime de liberté à un cadre plus restrictif.

b) Aux Etats-Unis : une protection réservée aux citoyens américains

La question de la légalité des écoutes aux Etats-Unis se ramène à celle de l'application aux activités de la NSA des dispositions de l'amendement n° 4 de la constitution américaine.

Les responsables américains, rencontrés par votre Rapporteur ou dont il a analysé les propos, ont indiqué que :

— la protection des citoyens est effectivement assurée par l'amendement n° 4. Celui-ci dispose que « *le droit pour le peuple d'être protégé… contre des perquisitions et saisies déraisonnables ne devra pas être violé* » ;

— les activités des agences fédérales américaines comme la NSA et la CIA sont soumises à cet amendement. Votre Rapporteur a déjà évoqué à ce propos les affirmations du porte-parole du département d'Etat James Rubin ou du directeur de la NSA devant les commissions spéciales du Congrès en charge du renseignement.

Il est nécessaire de souligner que, dans ce cadre :

— la protection contre les intrusions ne concerne sans ambiguïté que les citoyens américains, c'est-à-dire les nationaux résidents sur le territoire national des Etats-Unis, comme l'ont souligné les propos tenus lors des auditions devant le Congrès au printemps dernier. La protection ne vise évidemment ni les citoyens ni les institutions des autres pays et un doute subsiste sur la situation des citoyens américains à l'étranger et des étrangers sur le territoire américain ;

— le contrôle parlementaire des agences fédérales américaines ne permet pas de connaître la nature exacte de leurs activités.

Comme l'ont rappelé les interlocuteurs de votre Rapporteur, les activités de la NSA –comme celles de la CIA- sont soumises à la constitution des Etats-Unis, aux lois fédérales, aux règlements pris par l'exécutif, et sont surveillées par deux instances, le *President's Intelligence Oversight Board* (IOB) et les commissions spéciales du Congrès qui ont

déjà été évoquées. En fait, il semble que le contrôle s'effectue au travers d'un autre organisme *l'Office of the Inspector General* (OIG) qui seul effectue les investigations nécessaires et adresse un rapport aux autorités parlementaires et gouvernementales. De plus, les informations les plus sensibles ne sont confiées qu'aux responsables de ces autorités et les auditions publiques des directeurs d'agences fédérales au Congrès ne permettent pas aux parlementaires américains d'obtenir des informations suffisantes sur les objectifs et l'activité réelle de ces agences.

c. Les systèmes de sécurité des communications en france

Le Gouvernement français semble définir peu à peu une politique plus volontariste en matière de sécurité des communications. Plusieurs volets concourent ainsi à renforcer cette sécurité :

— d'une part, la consolidation de l'arsenal juridique et technique dans le cadre de la protection des données ou des atteintes à la vie privée face aux intrusions ou au piratage.

Tout d'abord, il convient de souligner la base constitutionnelle que représente le principe de liberté personnelle reconnu par le Conseil constitutionnel en se référant aux principes fondamentaux reconnus par les lois de la République dans le préambule de la constitution de 1946.

Par ailleurs, l'article 226-1 du Code pénal punit d'un an d'emprisonnement et de 300 000 francs d'amende « *le fait, au moyen d'un procédé quelconque, de porter atteinte à l'intimité de la vie privée d'autrui, en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel* ». De plus, la loi du 10 juillet 1991 relative au secret des correspondances émises par les télécommunications garantit les particuliers contre les interceptions de leurs communications, notamment au travers de l'action de la commission nationale de contrôle des interceptions de sécurité (CNCIS).

— d'autre part, l'encouragement sur un plan national au développement des moyens de confidentialité et de d'intégrité des SIC;

— enfin, remédier aux utilisations préjudiciables des technologies de l'information ne peut se concevoir que dans un cadre juridique international qui concilie à la fois la souveraineté des Etats et la protection des libertés individuelles. En effet, les écoutes reflètent un manque de déontologie de la part de certains Etats que seules des discussions multilatérales permettront de supprimer. C'est ainsi que, au plan européen, des négociations sont en cours dans le cadre du IIIème pilier de l'Union

européenne (Justice, Affaires intérieures) visant à harmoniser les droits nationaux et la coopération en matière de criminalité de haute technologie. D'autres enceintes comme le G 8 commencent à aborder cette question comme le montre le sommet spécifique sur la criminalité informatique de mai 2000 à Paris.

1. L'évolution récente des dispositifs

a) La libéralisation de la cryptologie : un nouveau cadre juridique

De manière générale, les dispositifs juridiques en matière de cryptologie distinguent plusieurs régimes en fonction de la finalité des moyens. Selon les cas (utilisation, fourniture, importation et exportation), quatre régimes sont concevables : la dispense de toute formalité (ou régime de liberté), la déclaration simplifiée, la déclaration et l'autorisation préalable.

La position des autorités françaises a profondément évolué depuis quelques années. La loi du 26 juillet 1996, complétée par les décrets du 24 février 1998 et des 13 et 23 mars 1998, a modifié le régime antérieur datant du début des années 90, en assouplissant les régimes de déclaration des produits de cryptologie et rendant entièrement libres les produits utilisant des clés de « 40 bits » qui sont soumis à simple déclaration. Mais, en 1996, privilégiant l'action des services de police et les nécessités d'ordre public, le Gouvernement refusait alors la libéralisation de la cryptologie des transmissions et imposait que les clés de chiffrement les plus performantes soient remises à un tiers habilité. Le système reposait sur l'habilitation donnée par le Service central de la sécurité des systèmes d'information et sur la remise des clés aux services compétents.

Ce nouveau cadre juridique a été récemment modifié. Le nouveau Premier ministre, M. Lionel Jospin, a en effet estimé que la possibilité de crypter les communications apparaissait comme une réponse efficace pour protéger la confidentialité des échanges et de la vie privée. Dans une déclaration à l'issue du Comité interministériel du 19 janvier 1999 pour la société de l'information, il a annoncé une modification du cadre législatif visant à offrir une liberté complète dans l'emploi des moyens de chiffrement pour les entreprises et les particuliers. Parallèlement il a souhaité des obligations afin que les autorités judiciaires, par exemple des juges d'instruction, puissent avoir connaissance, non pas des clés de déchiffrement, mais des copies en clair des messages cryptés.

La nouvelle réglementation repose sur trois axes : la libéralisation

d'outils de cryptage performants, les restrictions à l'exportation des systèmes performants et les poursuites pénales.

Les décrets n° 99-199 et n° 99-200 du 17 mars 1999 précisent ainsi que :

— l'utilisation de matériels et de logiciels de cryptologie dont la clé est inférieure ou égale à 40 bits est libre ;

— l'utilisation de matériels et de logiciels de cryptologie dont la clé est supérieure à 40 bits et inférieure ou égale à 128 bits est soumise à simple déclaration de leur producteur, de leur fournisseur ou de leur importateur ou s'ils sont exclusivement destinés à l'usage privé d'une personne privée. L'arrêté du 17 mars 1999 précise « *la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie* ».

Le Gouvernement a annoncé qu'il présenterait au Parlement une réforme plus complète offrant une liberté dans l'utilisation des produits de cryptologie (sous réserve du maintien des contrôles à l'exportation pour les moyens dotés d'une clé à 56 bits et au-delà) et ouvrant le recours à des tiers de confiance selon un régime facultatif (et non plus obligatoire).

La contrepartie à cette libéralisation de la cryptologie pourrait prendre plusieurs formes :

— une solution juridique à travers l'instauration d'obligations, assorties de sanctions pénales, pour remettre aux autorités judiciaires, lorsqu'elles en font la demande, de la transcription en clair des messages chiffrés. Il est en effet nécessaire d'empêcher les obstacles aux procédures judiciaires et de prévoir des sanctions fortes en cas d'absence de coopération des utilisateurs ou des détenteurs de clés avec l'autorité judiciaire ;

— des moyens nationaux dans les domaines de la cryptologie afin de maintenir une compétence face à l'évolution rapide de la technologie ;

— un renforcement des moyens des services de renseignement.

En outre, de par leur nature, la lutte contre la corruption et les écoutes inégales ressortissent de conventions internationales (par exemple, celle de l'OCDE) qui doivent être traduites en droit interne. La lutte contre le crime organisé, en particulier dans le cyberespace (identification des délinquants), suppose un cadre de référence international car il faut résoudre la contradiction entre les impératifs de libertés individuelles et les besoins

d'investigation et de coopération judiciaire ou policière.

b) Le développement des moyens de confidentialité et d'intégrité

L'encouragement sur un plan national au développement des moyens de confidentialité et de d'intégrité des systèmes de communication s'accompagne d'actions de sensibilisation et de d'information auprès des acteurs les plus sensibles. Elle s'est appuyée par la mise en place au début de 2000 d'un centre de veille, de prévention et de secours pour coordonner les efforts des administrations publiques.

Les PME sont encore plus vulnérables que les groupes aux interceptions et à l'espionnage économique. C'est pourquoi l'une des missions principales de la direction de la sécurité du territoire (DST) au ministère de l'Intérieur consiste à sensibiliser les partenaires scientifiques et économiques, à leur prodiguer des conseils, à effectuer (gratuitement) des audits ou des repérages des systèmes informatiques. Selon les interlocuteurs de votre Rapporteur, les plus réticents aux enjeux de sécurité restent les scientifiques et les universitaires pour lesquels les échanges (en particulier par voie informatique) sont essentiels sur le plan professionnel.

Ce travail de sensibilisation contribue à la défense du patrimoine scientifique et technologique. Il est essentiellement assuré par les services déconcentrés de la DST. Les conseils ne portent que sur les aspects défensifs. La DST agit sur sollicitation mais elle s'autosaisit dans les cas qui lui paraissent mériter l'attention. Elle a ainsi acquis une compétence reconnue au niveau interministériel.

Mais les moyens de la France sont trop dispersés, à l'image de l'éclatement de ses services spécialisés.

Il serait indispensable de créer une agence française dans le domaine de la sécurité des systèmes d'information. Elle serait rattachée au Premier ministre car sa vocation est interministérielle. Le regroupement des équipes existantes dans les différents services de renseignement permettrait d'atteindre une « masse critique ». La création de la DCSSI au SGDN pourrait préfigurer une telle agence. C'est pourquoi il a paru important à votre Rapporteur d'apporter des précisions sur l'évolution de cette structure.

c) Les programmes de protection

La France s'est laissée distancer dans les domaines de l'électronique et de l'informatique. Le plan Calcul a été un échec et aucun leader informatique n'existe en Europe qui subit de ce fait l'évolution

technique dans ces deux domaines alors qu'elle dispose d'excellents moyens d'expertise.

Alors que les Etats-Unis ont investi dernièrement près de 3 milliards de dollars sur trois ans en faveur de la sécurité des systèmes d'information, la France ne consacre qu'1 % de cette somme. Le montant des études amont sur ces questions a été doublé dans le budget 2000 (environ 40 millions de francs) mais cette dotation reste largement insuffisante. Le plan de charges actuel des organismes qui travaillent sur la cryptographie et la cryptanalyse, comme le CELAR de la DGA à Rennes, supposerait un doublement voire un triplement de leurs effectifs. Ainsi, le traitement des écoutes nécessiterait un effectif d'environ 1 000 personnes alors que seules 300 y sont affectées.

Mais il y a une double difficulté à garder les spécialistes (ingénieurs et universitaires contractuels), qui sont attirés par des emplois civils mieux rémunérés, et à embaucher de jeunes universitaires de haut niveau pour faire face à la demande. Face à cette pénurie, les services français ont été contraints de faire travailler sur contrats des spécialistes russes. La Russie a acquis un bon niveau dans la cryptographie et la cryptanalyse, mais les matériels produits manquent de fiabilité. Il manque également un grand projet pour animer les équipes françaises et leur donner des perspectives intéressantes.

Il faudrait travailler davantage sur le traitement des logiques sémantiques et en linguistique. Les progrès réalisés dans la reconnaissance automatique de langages et dans la traduction méritent d'être poursuivis. Il faudrait également augmenter les moyens de calcul mathématique.

Plusieurs industriels français (SAGEM, Thomson-CSF, Alcatel, Bull) disposent de réelles capacités dans les domaines des logiciels et de la cryptographie. L'essentiel de l'innovation provient cependant des *start up*. Les Etats-Unis savent aider au démarrage de ces petites entreprises en accord d'ailleurs avec les groupes. En France, les handicaps se cumulent dans la mesure où on ne prend pas assez de risques pour aider les petites entreprises innovantes et où certaines affaires douteuses ont incité les autorités à renforcer les contrôles sur les marchés publics. L'attention s'est donc plus portée vers un renforcement des contraintes du Code des marchés publics que vers leur assouplissement. Or ce code est inadapté à la taille et au domaine d'activité des *start up* notamment dans le domaine de la recherche.

Même si la question n'est pas de rattraper le retard pris sur les

partenaires d'Echelon grâce aux performances des nouveaux matériels, les moyens à mettre en œuvre sont incompatibles avec la réduction des budgets d'équipement. L'exemple français est même caricatural. Au moment où les enseignements de la participation des forces armées aux conflits du Golfe et de l'ex-Yougoslavie montrent la nécessité de la maîtrise de l'information, on a érodé les efforts financiers depuis le milieu des années 90 et les lois de programmation militaire ont été obérées par les grands programmes d'armement. La préparation de la prochaine loi de programmation militaire fournit l'occasion, en ce qui concerne les équipements militaires, de remédier à une situation incompatible avec l'ambition de la politique de sécurité des systèmes d'information.

2. Le SGDN et la sécurité des systèmes d'information

a) Les missions confiées au SGDN

Depuis 1996, le Secrétariat général pour la défense nationale (SGDN) est l'autorité interministérielle chargée d'assurer une double mission :

— veille sur le thème de la sécurité et information du Gouvernement ;

— impulsion de la politique gouvernementale pour favoriser la protection des réseaux et l'adaptation des moyens aux nouvelles technologies.

La protection des réseaux de communication a été favorisée par l'évolution de la réglementation sur la cryptologie. Pour le SGDN, des clés de chiffrement jusqu'à 128 bits offrent une excellente sécurité car elles sont très difficiles à briser. L'objectif demeure d'une libéralisation complète des produits de chiffrement sans limites de bits. Un projet de loi à cet effet sera présenté en 2000 au Parlement. L'une des conséquences sera cependant l'impossibilité pour les services de l'exécutif d'intercepter les communications pour les besoins de la sécurité nationale. Il en sera de même pour l'autorité judiciaire par les besoins des procédures pénales. C'est pourquoi des dispositifs doivent être prévus pour avoir accès aux clés lors de procédures judiciaires.

La montée en puissance des moyens du SGDN vise à accroître :

— l'expertise et les compétences dans les secteurs de la sécurité des systèmes d'information y compris au niveau de la recherche fondamentale ;

— les capacités opérationnelles d'évaluation et de réaction face aux menaces.

L'émergence d'une capacité interministérielle s'est accompagnée de la création en 1986 du service central de la sécurité des systèmes d'information (SCSSI), chargé d'apprécier le niveau de protection des systèmes d'information de l'Etat et de coordonner les études et développements dans le domaine de la sécurité des systèmes d'information. Les attributions du SGDN en matière de sécurité des systèmes d'information ont été précisées par le décret n° 96-67 du 29 janvier 1996.

La compétence du SGDN s'est accrue avec le rattachement en 1996 non seulement du SCSSI mais également de deux autres structures, le directoire interministériel et la commission interministérielle de la sécurité des systèmes d'information. L'intégration des moyens humains et budgétaires est achevée par le décret du 14 avril 1999. La transformation du SCSSI en direction centrale (DCSSI) sous l'autorité du SGDN consacre la prise de conscience de la vulnérabilité des systèmes d'information et de communications.

b) Les missions et les moyens de la DCSSI

Les missions essentielles de la DCSSI sont les suivantes :

— contribuer à la **définition** et à **l'expression d'une politique gouvernementale**, cohérente et prospective, en matière de sécurité des systèmes d'information.

Dans cette fonction, le SGDN anime les réflexions des structures publiques et assure le secrétariat des instances qui définissent la politique d'adaptation des moyens existants aux nouvelles technologies.

Il n'existe pas encore de politique coordonnée au niveau des différents pays européens. Seuls sont organisés des échanges avec les principaux d'entre eux. Mais la question des transferts des produits à l'intérieur de l'Union européenne devra faire l'objet d'une directive.

Par ailleurs, la relative atonie du secteur industriel français dans la production de biens de sécurité incite à la mise en place d'une politique publique du soutien à ce marché (favoriser des commandes publiques par exemple) ;

— assurer une **fonction d'autorité nationale de sécurité**.

La DCSSI délivrera des agréments ou des certificats pour les systèmes, les procédés et les produits de cryptologie employés par les services de l'administration et les services publics, l'Etat devant plus généralement assurer une surveillance du marché des produits de chiffrement pour vérifier qu'ils ne sont pas « piégés » mais bien conformes aux spécifications. Il ne s'agit pas du contrôle de ce marché (seules les exportations sont soumises à contrôle) mais de l'évaluation de la qualité de la protection qu'offrent ces produits ;

— **évaluer les menaces, donner l'alerte et développer les capacités pour les contrer**.

A la suite du comité interministériel pour la société de l'information du 19 janvier 1999, le Premier ministre, M. Lionel Jospin, a annoncé la création d'une structure d'alerte et de réponse aux attaques informatiques pour l'administration : le CERT/A (centre de recensement et de traitement des attaques informatiques) s'inscrit dans le réseau mondial des CERT (*computer emergency response team*) chargés de détecter les incidents informatiques et de résoudre les difficultés qu'ils peuvent entraîner ;

— développer **l'expertise technique** au bénéfice des administrations et des services publics afin de servir de pôle de référence pour la protection des systèmes publics.

Les compétences actuelles du SCSSI lui permettent d'effectuer des démonstrations d'attaques des réseaux publics pour faire prendre conscience aux administrations de la réalité des risques d'intrusion ou d'attaques de leurs réseaux et de l'urgence de leur sécurisation. En effet, la plupart des structures publiques n'ont pas de tradition du secret ni de culture de la sécurité hormis les ministères de l'intérieur, des Affaires étrangères ou de la Défense. Les ministères n'ont pas conscience de leur vulnérabilité ni de l'évolution des problèmes liée à l'évolution des techniques, des moyens et des acteurs. Ils font parfois preuve « d'imprudence et de candeur ». Il est donc nécessaire de les inciter à utiliser des messages sécurisés.

Les capacités dans ce domaine sont encore trop faibles surtout en comparaison des efforts réalisés en Allemagne ou au Royaume-Uni. Des dotations budgétaires supplémentaires sont nécessaires pour augmenter les moyens humains (ingénieurs et techniciens). Une véritable politique de recrutement d'équipes de spécialistes devient indispensable. Bien plus, elle devra s'accompagner du développement d'une culture de la sécurité.

III. — la réaction européenne au système Echelon

A. L'intérêt exprimé pour la question au sein des instances européennes

C'est essentiellement au nom de la défense des libertés publiques individuelles et des Droits de l'homme que le Parlement européen s'est saisi, depuis plusieurs années, du dossier des techniques de surveillance des moyens de communications modernes.

Face aux interrogations des parlementaires européens, la Commission a plutôt fait preuve d'un silence embarrassé.

1. Les travaux du Parlement européen

Dès 1997, la Commission des Libertés publiques et des Affaires intérieures du Parlement européen, devenue en juillet 1999 Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures (LIBE), a demandé une étude à l'Office des choix technologiques du Parlement européen. Celle-ci a tout d'abord fait l'objet d'un premier rapport publié en septembre 1998 « *Evaluation des techniques de contrôle politique* », qui a en fait été rédigé par la fondation OMEGA de Manchester, puis de quatre rapports déposés d'octobre à décembre 1999 et recensant les nouvelles technologies de communication, leurs risques et les moyens pour y remédier.

Auparavant, le Parlement avait adopté le 16 septembre 1998, une première résolution sur les relations transatlantiques dont les derniers paragraphes visent explicitement le système Echelon. Le Parlement européen demande que les 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* ». Il réclame l'adoption d'un code de conduite destiné à garantir la réparation d'erreurs ou d'abus. Il 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 massive appellent l'adoption de mesures de protection des informations économiques et d'un cryptage efficace* ».

Certains documents du STOA ont utilisé comme sources les ouvrages de James Bamford, Nicky Hager et Duncan Campbell que votre Rapporteur a déjà évoqués, ce qui montre une fois de plus que l'information

à propos d'Echelon circule « en boucles ».

a) Le rapport sur l'état actuel de la surveillance électronique

Ce premier document, qui a été rédigé par le journaliste britannique Duncan Campbell, évoque les nouvelles technologies utilisées et attire l'attention sur les cibles visées par les interceptions globales. Il montre que, depuis la naissance de la recherche électronique de communication, il y a eu une véritable évolution dans les moyens d'interception devenus de plus en plus sophistiqués. Il est vrai que les progrès liés à la cryptographie sont de plus en plus intégrés dans les télécommunications.

La recherche électronique de communication constituant, en grande partie, une activité industrielle, la plupart des nations développées la pratiquent, mais l'acteur le plus important en ce domaine est l'organisation UKUSA des nations anglophones. Le rapport contient aussi de nouvelles informations sur le système Echelon, dont il indique qu'il permet une surveillance du monde entier et vise essentiellement des cibles non militaires.

L'étude rappelle également l'historique des différentes réglementations applicables et montre la prédominance des Etats-Unis qui, selon l'auteur, ne va pas dans un sens propice au respect de la confidentialité et donc de la vie privée.

Le rapport évoque enfin les politiques possibles en matière de surveillance électronique.

b) Le document sur les techniques permettant de lutter contre les formes d'interception

Le but de ce rapport est de décrire les principales techniques qui permettent de se préserver contre toutes formes d'interception technologique des communications. Il a été rédigé par Franck Leprevost, professeur à l'université technique de Berlin.

L'étude reprend les différents types de technologies qui sont apparues en matière de télécommunications et leurs risques, puis donne une description des techniques de cryptographie et de chiffrement. Il montre que la surveillance électronique, qui permet bien souvent de protéger la sécurité nationale, connaît aussi certains effets pervers comme l'espionnage industriel. L'auteur 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 a pour objet de mettre au point des techniques et des modes d'intrusion pour réduire la sécurité

théorique d'algorithmes cryptographiques. Il traite à ce propos de la cryptanalyse quantique, qui recouvre l'ensemble des techniques permettant de trouver les clefs secrètes de protocoles cryptographiques à l'aide d'ordinateurs quantiques.

En raison de l'importance des conséquences politiques, diplomatiques et financières de la cryptanalyse et de la cryptographie quantique, différents pays dont la France ont signé plusieurs accords pour contrôler ces procédés. Le dernier en date est l'accord de Wassenaar, dont le document de M. Franck Leprevost commente la partie : *« Sécurité de l'information »* et analyse les conséquences.

L'accord de Wassenaar établit 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 institue un contrôle de l'exportation des procédés de cryptographie en tant que biens à double usage, mais il 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, seules 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. Le rapport de Franck Leprevost suggère des options possibles aux institutions européennes pour mettre en place une réglementation 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 interceptées et décodées par le réseau Echelon.

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

c) L'étude sur la légalité des interceptions

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

Il présente 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 ne dit pas que les interceptions légales sont interdites mais seulement celles réputées arbitraires. L'Union européenne a ainsi pu adopter une législation permettant aux Etats 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 ratifiées en n'interdisant pas les interceptions légales non arbitraires. Quant aux Etats membres, ils ont 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 expose succinctement les législations nationales existantes en matière d'interceptions.

d) L'analyse des risques possibles des interceptions et la vulnérabilité du commerce électronique

Le quatrième rapport a été effectué par le cabinet d'études ZEUS (Groupement d'intérêt économique européen), situé à Patras, sous la direction de M. Nikos Bogonikilos. Son but a été d'examiner l'utilisation des interceptions légales de communication et de mettre en évidence leurs risques possibles.

Il est organisé en trois parties : les options possibles ; les informations disponibles (avis d'experts) ; un dossier technique sur les nouvelles technologies.

Certaines options politiques y sont proposées, comme la mise en place d'un réseau global pour les communications. Le rapport contient des recommandations relatives aux capacités techniques permettant de protéger l'anonymat des communications. La faisabilité de ces capacités a été vérifiée auprès d'experts, tous d'accord aujourd'hui pour dire que presque toutes les informations économiques s'échangent par voie électronique (90 % d'entre eux estiment que, malgré les différentes législations, il existe encore des activités illégales de surveillance électronique et que, depuis le développement d'Internet, l'augmentation des transactions électroniques a fait naître le besoin d'un encadrement stable pour les relations

commerciales).

Le dossier technique donne une vision d'ensemble de la surveillance électronique. Une liste non exhaustive des organisations qui la pratiquent est mise en avant, la plus importante étant l'organisation UKUSA.

La nature des informations recueillies par les interceptions n'est pas sans incidence sur l'appréciation des effets et du but de ces activités. Si les interceptions des communications sont effectuées dans un but de défense nationale ou de lutte contre la criminalité, moins de problèmes se posent, mais si les informations recueillies sont utilisées dans un intérêt économique, certains risques peuvent survenir, comme celui d'abuser de ces informations. Des exemples sont donnés par cette étude, qui illustrent bien ces dangers. Mais le progrès technique ne va pas seulement dans un sens (permettre que les interceptions soient de plus en plus faciles), de nouveaux systèmes de protection s'étant aussi développés.

L'étude dresse un historique de la réglementation en vigueur. C'est d'abord en Europe qu'une législation pour la protection de la vie privée a vu le jour, le respect de la confidentialité y étant 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 pour faire accepter et adopter sa position par d'autres Etats. 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.

e) La constitution d'une commission parlementaire

A la suite de la parution de ces rapports et des travaux de la Commission des libertés et des droits des citoyens, le groupe politique des Verts a demandé la création d'une commission temporaire d'enquête sur proposition du député européen Paul Lannoye. Bien qu'un nombre suffisant de signatures ait été réuni, la création de la commission d'enquête a été refusée par le Parlement européen qui, sur proposition de sa conférence des présidents, a décidé, le 5 juillet 2000, la création d'une commission parlementaire temporaire de 36 membres sur le même sujet.

La différence entre les deux structures n'est pas si fondamentale puisque leurs attributions et leurs mandats sont fixés et que le calendrier de leurs travaux est limité dans le temps (un an pour les deux types de commission selon les articles 150 et 151 du Règlement du Parlement

européen). La commission d'enquête aurait peut-être un aspect politique plus marqué que la commission temporaire qui représente un compromis entre les groupes politiques du Parlement européen et s'apparente à une commission permanente sans toutefois disposer de moyens d'investigation spécifiques.

Le mandat de la commission temporaire, qui marque la volonté du Parlement européen de collaborer avec les parlements nationaux sur Echelon, a été ainsi défini :

« *— vérifier l'existence du système d'interception des communications connu sous le nom d'Echelon et dont l'activité est décrite dans le rapport STOA sur le développement des technologies de surveillance et le risque d'abus d'informations économiques ;*

— vérifier la compatibilité d'un tel système avec le droit communautaire, en particulier l'article 286 du traité CE et les directives 95/46/CE et 97/66/CE, et avec l'article 6, paragraphe 2, du traité sur l'Union européenne, sur la base des questions suivantes :

les droits des citoyens européens sont-ils protégés contre les activités des services secrets ?

Le cryptage constitue-t-il une protection adéquate et suffisante pour protéger la vie privée des citoyens ou faut-il prendre des mesures complémentaires et, dans l'affirmative, de quel ordre ?

Comment renforcer la prise de conscience des institutions européennes à l'égard des risques suscités par ces activités, et quelles mesures peut-on prendre ?

— vérifier si l'interception des communications au niveau mondial fait courir des risques à l'industrie européenne ;

— proposer, le cas échéant, des initiatives politiques et législatives ».

2. Le silence embarrassé de la Commission

A de nombreuses reprises, les députés européens ont posé des questions écrites ou orales relatives au système Echelon. Les réponses de la Commission Santer, notamment de la part de Sir Leon Brittan, alors commissaire, ont toujours manifesté un certain embarras. Soit la Commission a répondu de manière un peu étonnante « *qu'elle ne disposait d'aucun élément* » ou « *d'aucune preuve de ces allégations* », à l'exception d'articles de presse. Soit elle a rappelé qu'elle n'avait été saisie d'aucune plainte mettant en cause l'un des Etats membres.

Le Commissaire Bangemann a même mis en doute l'existence d'Echelon lors d'une déclaration, le 14 septembre 1998, ajoutant cependant que « *si ce système existait, tel que décrit, il s'agirait effectivement d'une violation, des droits individuels du citoyen et d'une atteinte à la sécurité des Etats membres* ».

Les commissaires ont cependant préconisé –à l'instar du Gouvernement français dans ses réponses aux députés ou aux sénateurs– une libéralisation des techniques de chiffrement pour protéger la confidentialité des communications.

La nouvelle Commission présidée par M. Romano Prodi n'a pas encore répondu aux questions posées par les Parlementaires européens sur Echelon et n'a fait aucune déclaration officielle sur le sujet.

B. Une position ambiguë

1. La mise en œuvre d'un système de surveillance européen

a) Les projets liés à la définition d'intérêts communs

Plusieurs sources font état d'un projet européen de surveillance des communications par téléphone ou par Internet dans le cadre du troisième pilier du traité de Maastricht relatif à la coopération dans les domaines de la justice et des affaires intérieures.

La finalité de ce système semble circonscrite. Le Conseil des Ministres de l'intérieur et de la Justice, s'appuyant sur la résolution du 17 janvier 1995 relative à l'interception légale des télécommunications, a approuvé, le 24 novembre 1995, un accord-cadre sur l'interception des

télécommunications dans le but de s'engager dans des standards d'écoute internationaux et de préparer une convention entre quinze pays. Selon le texte adopté, les opérateurs devront faciliter l'accès à la totalité des télécommunications transmises, donner accès à toutes les données associées, garder les clés des systèmes de chiffrement, intégré ou non au réseau.

Selon l'organisation *Statewatch*, basée au Royaume-Uni, le texte de la résolution s'inspire étroitement des dispositions proposées par le FBI, ce qui incite à imaginer une filiation directe entre les systèmes d'écoutes aux Etats-Unis et les textes en préparation dans le cadre de l'Union européenne.

En fait, l'Union européenne est placée devant un dilemme. Soit elle refuse les propositions des Etats-Unis sur les modalités techniques des interceptions, risquant ainsi de se priver d'une source considérable d'informations, en particulier dans le cadre de l'assistance mutuelle en matière criminelle. Soit elle accepte de telles interconnexions au risque de voir consolider la prédominance américaine sur l'ensemble des réseaux, et de ne plus pouvoir neutraliser d'éventuelles intrusions de la part des Etats-Unis.

b) Les limites à l'élaboration d'un système commun

La question a été posée de la création d'un réseau au niveau européen et du développement des échanges de renseignement entre partenaires de l'Union.

Pour cela plusieurs conditions paraissent nécessaires. Il conviendrait tout d'abord d'instaurer un contrôle politique commun des services de renseignement et de partager une culture du renseignement. Ainsi, si les parlementaires nationaux souhaitent disposer d'informations confidentielles, les gouvernements qui les communiqueront voudront s'assurer que ces parlementaires sauront les garder secrètes.

Or cette approche est différente selon les pays. En Allemagne, par exemple, le débat a été très vif au moment de la création de la commission parlementaire de contrôle qui autorise les actions du service fédéral de renseignements (BND). C'est pourquoi, alors que même des députés d'opposition peuvent avoir accès en Allemagne à des informations confidentielles, cette pratique suppose une restriction du droit de parole des élus. Les parlementaires SPD et Verts estiment que les opérations des services secrets doivent demeurer secrètes, mais que les règles de fonctionnement et les dotations financières de ces services peuvent être rendues publiques.

De nombreux obstacles s'opposent par ailleurs à l'établissement d'un réseau européen d'interception des communications :

— La nature même du renseignement

Le renseignement reste toujours sous responsabilité nationale. Pour envisager un réseau commun, il faudrait accepter que les pays coopèrent sur un domaine considéré comme relevant de leur souveraineté.

Certes, des moyens communs peuvent être mis en place, comme le montre l'exemple du satellite d'observation spatiale Helios I, dont les images sont partagées entre les trois pays participant au programme, selon une clé qui reflète leur part dans le financement (Espagne 7 %, Italie 14 %, France 79 %). L'exploitation des données doit cependant répondre à une politique unique. C'est là l'une des principales faiblesses des institutions communes comme le centre satellitaire de l'UEO à Torrejon en Espagne, le manque de vision commune empêchant d'aller au-delà de la mise en commun de certains équipements.

De plus, les pays restent « protectionnistes » en matière de cryptologie, car ils souhaitent conserver leurs compétences technologiques dans ce domaine et ne veulent pas devenir dépendants.

— Les différences de culture de renseignement

Cet argument a été mis en avant par de nombreux interlocuteurs de votre Rapporteur au cours de ses entretiens.

Deux pays, comme la France et le Royaume-Uni, qui ont une longue tradition de services de renseignement, s'opposent sur l'image différente du renseignement dans l'opinion publique. En France, le renseignement a une connotation souvent péjorative, ses réussites sont tues et il est souvent assimilé aux services d'action dont les échecs sont médiatisés. Le Royaume-Uni a en revanche su cultiver auprès de ses élites une image valorisante de la communauté du renseignement.

Plus la proximité culturelle est grande entre pays, plus il est facile de s'allier sur des sujets sensibles comme le renseignement. Les relations de connivence qu'entretiennent souvent les pays anglo-saxons favorisent ce type d'alliance.

— La dispersion des centres de décision

L'organisation qui dirige le réseau Echelon est centralisée et reste sous contrôle politique. En France, le renseignement est réparti entre plusieurs structures, dépendant des ministères de l'Intérieur (DST) ou de la Défense (DGSE, DPSD et DRM) sans véritable « chef d'orchestre ». Le SGDN assure néanmoins une coordination qui s'est renforcée depuis la nomination de Jean-Claude Mallet.

Contrairement aux Etats-Unis et à l'exception de la Grande-Bretagne, les pays européens s'engagent peu sur les enjeux de la maîtrise et de la sécurité de l'information. Pourtant une vision européenne est concevable dans les domaines du renseignement et de la cryptologie.

Un système européen ne peut guère être envisagé mais deux possibilités restent concevables, l'une pour la gestion des clés, l'autre dans l'élaboration de standards et de logiciels communs afin d'éviter les intrusions dans les systèmes.

Les limites d'une politique commune sont liées à la nécessité d'effectuer des investissements importants et d'inciter les utilisateurs à privilégier ces nouveaux équipements. La gestion commune des systèmes de clés se heurte à la forte concurrence entre entreprises des différents pays et au maintien des particularismes nationaux.

L'amorçage d'une politique commune pourrait venir d'une coopération bilatérale entre la France et l'Allemagne qui attirerait ensuite les pays intéressés notamment la Grande-Bretagne et les pays scandinaves. Les capacités technologiques et financières existent, la volonté politique paraît moins acquise.

2. Les perspectives ouvertes par la politique européenne de sécurité et de défense

La construction de l'Europe de la défense comportera de manière inévitable un volet relatif au renseignement et conduira à de nouvelles relations entre membres de l'Union européenne notamment avec le Royaume-Uni. Une réflexion est d'ailleurs engagée dans ce pays sur la mise en commun du renseignement tout en maintenant un lien spécifique avec les Etats-Unis. Le développement de la coopération est cependant indissociable de la confiance entre partenaires car il n'y a pas de vérification possible entre eux. Les suspicions et les doutes doivent s'effacer.

Le sommet d'Helsinki a mis en avant un objectif de capacités collectives, y compris dans le renseignement. Le sommet de Mayence a montré que l'Allemagne avait repris l'initiative et souhaitait développer de nouveaux moyens (satellites radars) et participer à un système européen d'observation par satellites. Le centre satellitaire de Torrejon sera vraisemblablement intégré dans l'Union européenne si celle-ci veut avoir un rôle plus actif dans la gestion des crises. Ce centre doit conserver ses capacités d'acquisition d'images et d'analyses mais de nouveaux moyens doivent lui être conférés si l'on veut qu'il serve les besoins collectifs de l'Union européenne.

A la suite des sommets européens et du sommet franco-allemand de Mayence, on peut imaginer plusieurs approches pour le développement de l'Europe de la défense. Le sentiment demeure qu'il faudrait privilégier l'entente entre quelques partenaires pour développer les échanges de renseignement, l'objectif étant de remettre aux instances de l'Union européenne un renseignement à usage militaire déjà élaboré. Dans le cadre des capacités satellitaires, il pourrait être envisagé une mise en commun ou une mutualisation des moyens nationaux de recueil. Pour les Ministres de la Défense, il est nécessaire de traduire les objectifs européens en capacités de forces, déterminer les contributions des différents Etats membres, et engager des discussions pour combler les manques qui pourraient apparaître.

L'évolution de la position allemande est due en grande partie au conflit du Kosovo dans la mesure où l'Allemagne a peu apprécié la rétention d'informations de la part des Etats-Unis, ce qui explique les propositions du Ministre allemand de la Défense. A une initiative du Chancelier Kohl non acceptée par le Ministre de la Défense Rühe succède une situation différente où l'initiative des Etats-majors allemands est relayée par la nouvelle Chancellerie.

CONCLUSION générale

Au terme de ses réflexions, votre Rapporteur aimerait rappeler un certain nombre des constats qu'il a effectués et formuler des propositions.

1. A partir de quelques certitudes sur Echelon…

Quelles sont tout d'abord les certitudes que votre Rapporteur vous demande de partager ?

Oui, il existe bien un vaste système d'interception et de traitement des informations nommé Echelon. Il est organisé en réseau. Il s'agit d'ailleurs du seul système multinational connu.

Oui, les capacités d'un tel système sont réelles et elles le rendent performant, compte tenu des multiples vulnérabilités des systèmes d'information et de communication. Le développement du réseau s'est appuyé sur le développement de compétences techniques et la mise en place de multiples installations. Il a bénéficié d'importants investissements en hommes et en équipements depuis près de quarante ans. Il faut cependant ajouter que les performances ont atteint leurs limites, non seulement parce que les moyens engagés ne sont plus en rapport avec l'explosion des communications dans le monde mais aussi parce que certaines cibles ont appris à se protéger des interceptions.

Oui, le système Echelon a "divergé" par rapport à ses objectifs initiaux, qui étaient fondamentalement liés au contexte de la guerre froide et par rapport même aux conditions du pacte initial UKUSA entre les cinq partenaires. Il n'est pas impossible que des informations recueillies soient utilisées à des fins politiques et économiques, voire à l'encontre de certains membres de l'Alliance atlantique. Si les preuves manquent pour évoquer l'espionnage industriel, les propos d'anciens responsables d'agences de renseignement constituent autant d'aveux.

Oui, des liens bilatéraux ont été organisés entre les Etats-Unis, l'UKUSA et d'autres services de renseignement pour des raisons de sécurité liées à des besoins militaires ou à la nécessité de lutter contre le terrorisme ou le grand banditisme.

Oui, Echelon peut constituer un danger pour les libertés publiques et individuelles. A ce titre, son existence pose de nombreux problèmes et

nécessite donc des réponses appropriées. En effet, il serait vain d'imaginer que les pays membres du réseau cessent leurs activités. Le système d'ailleurs évolue et s'adapte. Plusieurs indices semblent inciter à croire qu'un nouveau système s'est constitué pour dépasser les limites d'Echelon grâce à de nouveaux moyens et sans doute de nouveaux partenariats.

2. …Quelles peuvent être des propositions concrètes pour diminuer les risques ?

Les constatations qui précèdent appellent l'application d'un principe général de précaution. Ce principe suppose que soient prises des mesures qui vont au-delà des premières mesures de prévention liées à la sécurité des systèmes d'information et de communication (SIC). Pour cela, plusieurs actions sont concevables. Elles constituent autant de propositions de votre Rapporteur :

— **l'information de tous les acteurs** sur les risques potentiels et leur sensibilisation constituent des préalables pour qu'ils prennent les mesures de protection nécessaires de manière adaptée. Il revient en priorité à ces acteurs de protéger leurs communications en ayant recours aux moyens de protection, dont la cryptologie n'est qu'un des aspects, et cela en fonction du degré de confidentialité qu'ils estiment nécessaire pour ces communications ;

— au sein de chaque structure constituant une cible potentielle des écoutes ou des attaques informatiques, il conviendrait de recommander la **formation de responsables de la sécurité** des systèmes de communication ;

— **la production de logiciels sûrs,** tant en matière de cryptographie que pour les applications bureautiques et informatiques**,** représente une condition essentielle de l'efficacité d'une riposte. Dans un premier temps, ces logiciels pourraient être nationaux mais on peut imaginer qu'ils seront européens à relativement court terme ;

— **la libéralisation des programmes de cryptographie** ou de chiffrement devient impérative. Elle pourrait être double. Non seulement le dispositif juridique français devrait autoriser la vente et l'utilisation de programmes d'une capacité de 128 bits mais les échanges qui supposent une plus grande confidentialité, comme l'échange de clés, devraient bénéficier d'une libéralisation accrue pour des produits d'une valeur supérieure à la limite de 128 bits qu'envisage le Gouvernement actuel (jusqu'à 1 024 bits par exemple) ;

— **la revalorisation des fonctions de renseignement** aurait pour but de faire naître dans notre pays une véritable culture du secret et du renseignement qui lui fait actuellement défaut. Elle pourrait s'inspirer de la considération dont bénéficie la communauté du renseignement dans les pays anglo-saxons, en particulier au Royaume-Uni ;

— **l'élaboration d'une véritable déontologie du renseignement** représente également un objectif essentiel pour protéger les libertés individuelles à tous les niveaux.

Les particuliers n'ont pas toujours les moyens ni n'éprouvent l'utilité de mettre en œuvre des mesures de protection de leurs communications alors qu'ils sont les premières victimes des atteintes aux libertés publiques. Il apparaît donc nécessaire que des accords soient conclus entre Etats afin d'élaborer un nouveau cadre juridique qui les rassure et les protège.

— enfin, **l'engagement de négociations internationales** apparaît indispensable dans un débat qui s'affranchit du cadre national.

Plusieurs niveaux sont concevables et les accords pourraient se négocier sur un mode bilatéral ou multilatéral afin de promouvoir une réelle avancée démocratique. Dans cette hypothèse, il pourrait être fait appel aux mesures de protection et de garantie qui concernent les citoyens américains et qui se verraient étendues aux citoyens européens pour lever toute ambiguïté.

Plusieurs enceintes sont susceptibles de servir de cadre à ces accords.

L'Union européenne est adaptée à la mise en place d'une réglementation commune en matière de cryptologie et de protection des données. Le niveau communautaire facilite également le dialogue avec le Royaume-Uni dont la position ambiguë devra être clarifiée.

Le cadre de l'OCDE ou celui du G 8, qui permettent d'associer les Etats-Unis et le Canada dans une réflexion élargie, visent tout autant à améliorer les services nationaux en matière d'enquêtes et de poursuites contre les nouvelles formes de criminalité qu'à définir les limites de la souveraineté des Etats dans les domaines qui concernent les impératifs de libertés publiques, la protection des droits de l'Homme et de la vie privée ainsi que la liberté des communications.

L'Alliance atlantique peut également fournir une solution dans la

mesure où le dialogue est particulièrement nécessaire entre alliés sur une question touchant des divergences entre eux.

— **le rôle des pouvoirs publics** dans tous ces domaines est essentiel car leur responsabilité consiste à la fois à proposer un dispositif juridique adapté, à sensibiliser les acteurs et opérateurs, à certifier les produits de protection et les systèmes qui permettent d'assurer la sécurité, et à acquérir une compétence d'expert.

Cette action multiple a déjà commencé en France sous la tutelle et le contrôle interministériels du SGDN. Des moyens nouveaux doivent lui être accordés afin qu'il assure sa mission de coordination et d'impulsion des services de l'Etat chargés de la protection des systèmes d'information et de communication.

Ainsi, à l'occasion d'une première réflexion sur les réseaux d'interception des communications et en particulier du système Echelon, se dessinent d'importantes réformes sur le plan national comme dans un cadre international : toutes supposent une nouvelle approche déontologique des Etats, qui concilie à la fois le respect de leurs impératifs nationaux et l'élaboration d'une même démarche.

examen en commission

La Commission a procédé à l'examen du rapport d'information de M. Arthur Paecht, rapporteur, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale.

M. Arthur Paecht a tout d'abord rappelé qu'à la suite de la parution de plusieurs rapports du Parlement européen sur le réseau Echelon et d'interrogations de l'opinion publique reflétées par la presse, la Commission de la Défense nationale avait décidé, le 29 février dernier, de lui confier un rapport d'information sur les « *systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale* ». La Commission avait également décidé d'associer à l'élaboration de ce rapport un groupe de travail dans lequel chaque groupe politique serait représenté. La nature du sujet abordé, qui ne pouvait être efficacement traité que un seul parlementaire n'a toutefois pas permis aux membres de ce groupe de travail de participer directement aux investigations du rapporteur.

M. Arthur Paecht, après avoir reconnu que cette situation avait pu faire naître un sentiment de frustration chez les membres du groupe de travail, a souligné qu'il avait d'abord voulu comprendre la nature exacte du réseau Echelon, analyser ses capacités réelles et évaluer ses véritables dangers, dans trois domaines en particulier : les risques qu'il comporte pour la sécurité nationale, les possibilités qu'il offre d'une utilisation à des fins économiques et l'atteinte aux libertés publiques individuelles qu'il pourrait permettre.

Il a indiqué qu'il s'était ensuite interrogé sur les raisons de la médiatisation actuelle du réseau Echelon et de l'intérêt subit manifesté pour les réseaux d'écoutes, se demandant si ces phénomènes n'étaient pas dus à des causes complexes s'apparentant à des manipulations. Il avait également souhaité comprendre l'attitude des gouvernements occidentaux non membres du pacte fondateur d'Echelon à l'égard des réseaux d'interception.

Enfin, il s'était interrogé sur les moyens qui permettraient de réduire la vulnérabilité des administrations, des services publics, des entreprises et des particuliers aux interceptions de leurs communications et s'est demandé quelle forme pourrait prendre une position commune des Etats de l'Union européenne face aux intrusions qui peuvent léser leurs intérêts.

Le rapporteur d'information a ensuite évoqué les difficultés

inhérentes au sujet et a regretté à cet égard la faiblesse des moyens dont dispose le Parlement pour mener des études sur un tel sujet. Il a souligné que l'objet de son rapport avait été considéré comme difficile par tous les interlocuteurs rencontrés, certains se félicitant cependant de l'intervention du Parlement et considérant que tout débat en cette manière était sain. Ce sont les rencontres souhaitées avec les responsables des services de renseignement qui ont soulevé les difficultés les plus grandes.

M. Arthur Paecht a fait observer qu'il s'était heurté en ce domaine à une fin de non-recevoir de la part des autorités américaines et britanniques. Le refus des autorités britanniques de permettre au rapporteur de rencontrer des responsables de leurs services de renseignement s'est fondé sur le fait qu'il n'était « *même pas membre d'une instance parlementaire chargée du contrôle des services de renseignement* ». Cette attitude ne peut que conforter la Commission dans l'idée que l'inscription à l'ordre du jour de l'Assemblée nationale de la proposition de loi visant à la création de délégations parlementaires pour le renseignement est plus que jamais nécessaire.

Aux Etats-Unis, la décision de l'administration fédérale, difficile à comprendre mais prise, semble-t-il, au plus haut niveau et après de nombreuses délibérations, de ne pas permettre de rencontre entre le rapporteur et des responsables des services de renseignement a comme conséquence de relancer toutes les suspicions sur les missions d'Echelon et en particulier sur le rôle qu'y jouent les Etats-Unis. Cette décision est d'autant plus surprenante que des responsables ou d'anciens responsables d'agences fédérales se sont exprimés publiquement sur le sujet. L'ensemble des interlocuteurs rencontrés à Washington a d'ailleurs exprimé son incompréhension vis-à-vis du refus des autorités américaines.

M. Arthur Paecht a alors fait part des principales conclusions auxquelles il était parvenu, soulignant qu'elles étaient dépourvues d'intention polémique et qu'elles reflétaient une conviction profonde :

— il existe effectivement un système d'interception des communications, mis en œuvre par les services de renseignement des Etats-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande. L'existence de ce système, qui s'est développé de manière spectaculaire dans les années 70 et 80, est attestée par le fonctionnement de bases ou de stations d'écoutes dans les cinq pays participants ainsi que sur le territoire d'autres Etats comme le Japon ou l'Allemagne (à Bad Aibling). Elle est confirmée par de nombreux témoignages et par certains documents rendus publics ;

— pour les créateurs de ce système, les enjeux de sécurité justifient son maintien. Or il n'est pas impossible que certaines informations recueillies puissent être utilisées à des fins politiques et économiques. Même si aucune entreprise française ne s'est plainte d'écoutes, dont aucune preuve ne semble d'ailleurs pouvoir être apportée, les aveux non démentis d'anciens responsables de services américains, au-delà de leur aspect provoquant et moralisateur, tendent à prouver que, dans certaines affaires citées par les médias et touchant des entreprises européennes, des interceptions ont bien bénéficié indirectement à des sociétés américaines ;

— les moyens acquis depuis quarante ans par les services de renseignement acteurs d'Echelon permettent de recueillir, sinon de traiter, un très grand nombre de communications. Cependant, l'explosion des communications et le développement des mesures protectrices, en particulier le chiffrement des messages, compliquent l'exploitation des données recueillies. L'obsolescence technologique prochaine des réseaux d'écoutes limite leurs capacités, les agences de renseignement étant dépassées sur un certain nombre de créneaux ;

— le débat s'est en fait déplacé de l'intrusion dans les réseaux de communications à l'intrusion dans les réseaux informatiques, c'est-à-dire au plus près de la source émettrice des messages, compte tenu de la vulnérabilité des systèmes informatisés de communication.

Devant ces évolutions, le rapporteur d'information a tout d'abord préconisé d'appliquer un principe général de précaution, au-delà des premières mesures de prévention liées à la sécurité des systèmes d'information et de communication. Il a en premier lieu souligné la nécessité d'informer tous les acteurs sur les risques potentiels et de les sensibiliser pour qu'ils prennent les mesures de protection nécessaires de manière adaptée. Il a insisté sur l'intérêt de recommander, au sein de chaque structure constituant une cible potentielle, la formation de responsables de la sécurité des systèmes de communication.

Il s'est prononcé en faveur de la production de logiciels sûrs, tant en matière de cryptographie que pour les applications informatiques, même si, dans un premier temps, ces logiciels pouvaient être nationaux avant de devenir à court terme européens. Il a également proposé une libéralisation des programmes de cryptographie ou de chiffrement de manière à autoriser la vente et l'utilisation de programmes d'une capacité de 128 bits. Quant aux échanges qui supposent une plus grande confidentialité, comme l'échange de clés, il a estimé qu'ils devraient bénéficier aussi d'une libéralisation accrue pour des produits d'une valeur supérieure à la limite de 128 bits

(jusqu'à 1 024 bits par exemple).

Enfin, après s'être prononcé en faveur d'une revalorisation des fonctions de renseignement qui ferait naître dans notre pays une véritable culture du secret et du renseignement, il a souhaité l'ouverture de négociations internationales dans un débat sur les systèmes électroniques de surveillance et d'interception qui doit s'affranchir du cadre national. Ces négociations, qui pourraient être à la fois bilatérales et multilatérales, auraient notamment pour objet de promouvoir un réel progrès des libertés démocratiques. Dans cette perspective, il pourrait être fait appel aux normes de protection dont bénéficient les citoyens américains et qui se verraient étendues aux citoyens européens.

L'Union européenne est adaptée à la mise en place d'une réglementation commune en matière de cryptologie et de protection des données. Des accords négociés dans le cadre de l'OCDE ou du G 8, qui auraient l'avantage d'associer notamment les Etats-Unis et le Canada, permettraient à la fois de renforcer l'efficacité des services nationaux en matière d'enquêtes et de poursuites contre les nouvelles formes de criminalité et de mieux protéger les libertés publiques. L'alliance Atlantique peut également fournir un cadre de négociation dans la mesure où le dialogue est particulièrement nécessaire entre alliés sur une question intéressant leur sécurité mais qu'ils abordent avec des préoccupations et des appréciations divergentes.

En conclusion, M. Arthur Paecht a souligné le rôle essentiel des pouvoirs publics pour proposer un dispositif juridique adapté, sensibiliser les acteurs et certifier les produits de protection ainsi que les systèmes qui permettent d'assurer la sécurité des communications. Il a également demandé que l'Etat consente un effort pour favoriser le développement de l'expertise en matière de sécurité des communications. Il a enfin proposé que des moyens nouveaux soient accordés au SGDN pour lui permettre de veiller à la coordination des actions des administrations dans le domaine de la protection des systèmes de communication.

Après s'être félicité de l'utilité du travail accompli, **le Président Paul Quilès** a souligné que la chute du mur de Berlin avait sans doute permis de réorienter largement le réseau Echelon vers l'espionnage économique, ce qui explique que les médias s'y soient intéressés dans la période récente, malgré l'ancienneté du système.

Alors que le discours moralisateur de certains Etats, qui œuvrent par ailleurs pour que rien ne change, ne débouche sur aucune action concrète, il convient sans doute de privilégier l'idée de protection plutôt que de tenter

de mettre en cause un système dont il est juridiquement difficile de contester l'existence. L'idée d'une régulation internationale de la surveillance électronique est intéressante mais elle se heurte à la concurrence des Etats et à l'opposition de leurs intérêts.

Tout en rappelant qu'il avait défendu le principe d'un rapport d'information sur le réseau Echelon, **M. Jean Michel** a regretté que le groupe de travail n'ait pas disposé de plus de pouvoir d'investigation et n'ait pas pu en particulier rencontrer des responsables des questions de surveillance électronique en activité. Il a demandé à ce propos que le Parlement exerce davantage les prérogatives que lui offre la Constitution, faisant ressortir le travail effectué par ailleurs par le Parlement européen.

Le Président Paul Quilès a souligné que le Parlement européen, qui se donnait peut-être un peu plus de temps, n'obtiendrait probablement pas des résultats très différents de ceux de l'Assemblée nationale. Il a rappelé que la Commission exerçait toutes ses prérogatives et qu'elle avait formulé de nombreuses propositions tendant à renforcer le rôle du Parlement dans le domaine de la politique de Défense. Il a à ce propos indiqué qu'il venait d'écrire au Premier ministre pour lui demander l'inscription à l'ordre du jour prioritaire du Gouvernement de la proposition de loi tendant à l'institution de délégations parlementaires pour le renseignement, adoptée par la Commission.

Reconnaissant l'importance du travail accompli par la Commission, **M. Jean Michel** a néanmoins souligné les limitations du contrôle parlementaire en France en comparaison d'autres démocraties.

S'agissant du système Echelon, il a observé que, pour la première fois sans doute, un réseau de renseignement travaillait non pour un pays mais pour un ensemble de nations appartenant au monde anglo-saxon (Etats-Unis et Royaume-Uni depuis 1943, Canada, Australie et Nouvelle-Zélande depuis 1947). Par ailleurs, Echelon, qui a tissé une « toile d'araignée » planétaire avec des emprises en Allemagne, au Japon et en Suisse, jouit de moyens considérables puisque plus de 70 000 personnes y collaborent dans un environnement culturel où l'action de renseignement bénéficie d'une image positive de patriotisme au contraire de la France.

Relevant que ce réseau, auquel contribuent peut-être de grands groupes du secteur de l'informatique et des communications, est présenté comme capable d'intercepter 180 millions de communications à l'heure, il s'est inquiété des atteintes qu'il porte inévitablement à la vie privée des particuliers, ne doutant pas que les grandes entreprises prenaient déjà de leur côté les précautions nécessaires.

Il a estimé, qu'eu égard à l'ampleur des questions soulevées, des investigations plus poussées étaient nécessaires.

M. Jean-Louis Bernard a confirmé le sentiment de frustration des membres du groupe de travail, précédemment évoqué par le rapporteur. Il a néanmoins estimé que la création d'une commission d'enquête n'aurait sans doute pas permis d'obtenir beaucoup plus d'informations que n'en avait reçu le rapporteur sauf, peut-être, auprès de responsables français. Jugeant positifs les résultats du travail accompli, il a souligné qu'il en avait retiré l'intime conviction que tout peut être écouté et stocké, même si le traitement des données rassemblées peut s'avérer difficile. Dès lors, la vie privée des individus est, plus que jamais, menacée car « les murs ont véritablement des oreilles ».

Après avoir estimé nécessaire de relancer les propositions de la Commission sur la création d'une structure parlementaire de contrôle des services de renseignement, il a fait remarquer que les responsables ou anciens responsables de ces services ne pouvaient qu'être embarrassés lorsqu'ils étaient interrogés sur un système avec lequel ils coopèrent, dans le cadre d'échanges d'informations, chaque organisme ayant coutume, en ce domaine, de « faire son marché » auprès des autres. Il lui est par ailleurs apparu particulièrement nécessaire de retenir que les produits informatiques, y compris ceux destinés au grand public, comportaient d'ores et déjà de nombreuses « trappes » à renseignements, estimant qu'un recours plus général aux techniques de cryptologie pouvait offrir une protection dont la portée restait toutefois à ce jour incertaine.

M. Arthur Paecht, rapporteur, a apporté les précisions suivantes :

— comme l'a souligné M. Jean Michel, le Parlement doit effectivement exercer pleinement ses pouvoirs en vue, tout particulièrement, d'assurer la protection des individus, les Etats et les grandes entreprises disposant quant à eux de certains moyens de défense ;

— la question du réseau Echelon ne saurait se résumer à une opposition entre le monde anglo-saxon et les autres pays. Les services de renseignement appartenant au noyau fondateur d'Echelon ont en effet noué des relations bilatérales étroites avec ceux de pays extérieurs au système, ne serait-ce qu'en raison des liens créés par l'Alliance Atlantique ou la construction européenne. Il a précisé que le monde asiatique, et notamment des pays comme la Chine ou le Japon, pouvaient eux aussi se doter de systèmes d'interception distincts, soit dans un cadre multilatéral, soit de manière plus autonome ou encore à partir de relations entretenues avec le

système Echelon ;

— à ce jour, seuls des parlementaires allemands ont pu visiter à Bad Aibling une station d'interception dans laquelle opèrent d'ailleurs les services de renseignement américains. Les autorités allemandes ont obtenu des Etats-Unis l'engagement de leur fournir les informations recueillies sur leur sol et de ne pas se livrer à des activités d'espionnage économique contre l'Allemagne. Elles ne disposent toutefois pas des moyens de vérifier le respect de cet engagement ;

— après avoir souligné avec satisfaction que la Commission pouvait confier des rapports d'information importants à des membres de l'opposition, il a fait valoir que le contrôle parlementaire était aussi affaire de volonté ;

— s'agissant des relations bilatérales nouées au profit de spécialistes français en marge du système Echelon, il a fait état de formations dispensées aux Etats-Unis dans le cadre d'une coopération mutuellement avantageuse.

La Commission a alors *autorisé* à l'unanimité la publication du rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale conformément à l'article 145 du Règlement.

annexe N° 1

LISTE DES PERSONNES RENCONTRÉES

AU COURS DE LA MISSION D'INFORMATION

Secrétariat général de la Défense nationale

— M. Jean-Claude Mallet, Secrétaire général de la Défense nationale

— Général Pierre-Jacques Costedoat, Secrétaire général adjoint

— Contre Amiral Jacques Gheerbrant

— Contre Amiral Stanislas d'Arbonneau

Ministère des Affaires Étrangères

— M. Régis de Bellenet, Directeur des affaires stratégiques, et M. Laurent Paillard, Conseiller auprès du directeur des affaires stratégiques

Ministère de la Défense

Délégation générale pour l'armement

— M. Jean-Yves Helmer, Délégué général pour l'armement

— M. Francis Chompret, Chargé de mission auprès du Délégué général

— M. Jean-Paul Gillyboeuf, Ingénieur général de l'armement

Direction du Renseignement Militaire

— Vice-Amiral Yves de Kersauson de Pennendreff, Directeur

— Lieutenant-Colonel Philippe Pengam, Chef de Cabinet

Direction générale de la Sécurité Extérieure

— M. Jean-Claude Cousseran, Directeur

Ministère de l'Intérieur

— M. Pierre Dabezies, Conseiller du Ministre de l'Intérieur pour les affaires de renseignement

Direction de la Surveillance du Territoire

— M. Jean-Jacques Pascal, Directeur

SAGEM

— M. Mazzenti, Directeur du développement

— M. Dupas, équipements de sécurité

Personnalités

— M. Guillaume Dasquié, Rédacteur en chef du **Monde du renseignement**

— Mme Anne-Marie Lizain, Sénatrice de Belgique

— M. Jacques Stern, Professeur à l'École Normale Supérieure

*

Mission à Berlin

— M. Ernst Uhrlau, Coordinateur pour les services de renseignement

— M. Hans-Jürgen Knoke, Vice-Président en charge de la sécurité de Deutsche Telekom

— M. Gerd Von Brandenstein, Vice-Président du groupe Siemens, chargé des relations avec le gouvernement et M. Alexander Von Erdmannsdorff, Directeur du groupe Siemens

— M. Karsten Voigt, Secrétaire d'Etat à la coordination des relations transatlantiques (germano-américaines)

— M. Niels et Mme Sigrid Hintzen, Conseillers juridiques du patronat allemand (BDI)

Mission à Washington

— M. Vernon Loeb, Journaliste au Washington Post

— M. Daniel Benjamin, *Senior Follow, US Institute of Peace*

— M. James Branford, Journaliste et écrivain

— M. Joan Grimson, *Deputy Majority Staff Director* du Sénateur Shelby, Président de la Commission spéciale du renseignement (*Senate Select Intelligence Committee*)

— M. Philippe Gordon, Directeur du Centre sur les Etats-Unis et la France – *Foreign Policy Studies Program*

— M. Porter J. Goss, Représentant, Président de la Commission spéciale du renseignement (*House* S*elect Intelligence Committee*)

— M. Andy Kutler, assistant du Sénateur Richard H. Bryan, vice-Président de la Commission spéciale du renseignement

— M. R. James Woolsey, Avocat, Ancien Directeur de la CIA

*

Déplacement au Centre électronique de l'armement à Rennes (CELAR)

annexe N° 2

COMPOSITION DU GROUPE DE TRAVAIL

— M. Arthur Paecht, rapporteur, député du Var (UDF)

— M. Jean-Louis Bernard, député du Loiret (UDF)

— M. Antoine Carré, député du Loiret (DL)

— M. René Galy-Dejean, député de Paris (RPR)

— M. Jean Michel, député du Puy-de-Dôme (S)

— M. Bernard Birsinger, député de Seine Saint-Denis (C)

— M. Aloyse Warhouver, député de la Moselle (RCV)

N° 2623.- Rapport d'information de M. Arthur Paecht, au nom de la commission de la défense, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale (Système Echelon).

1 *La composition de ce groupe de travail figure en annexe.*
2 *Ce premier accord, dénommé BRUSA, aurait été signé en mai 1943. Il aurait contribué à standardiser les méthodes et les procédures des services britanniques et américains en charge du renseignement électromagnétique.*
3 *La Nouvelle-Zélande n'aurait ainsi fait partie du réseau qu'en 1989 avec la construction de la base de Waihopaï.*
4 *Cette station ne fonctionne plus.*
5 *La qualification de station d'écoutes et d'espionnage a été reconnue par le Ministre britannique de la Défense dans une réponse parlementaire du 29 mars 1994.*
6 *Commission permanente sur le renseignement de la Chambre des Représentants (House Permanent Committee on Intelligence) et commission homologue du Sénat (Senate Permanent Committee on Intelligence)*
7 *Le premier du 17 mars 2000 dans le Wall Street Jornal, le second du 28 mars dans Le Figaro.*
8 *Ces manchons sont équipés de bobines qui capteraient les champs électromagnétiques émis par le câble. Un manchon récupéré par les Soviétiques aurait été exposé au musée du KGB à Moscou dans les années 80.*
9 *La barrière de la langue a rarement constitué une difficulté majeure dans l'histoire. Les méthodes employées par Thomas Young et Jean-François Champolion au XIXème siècle pour le déchiffrement des hiéroglyphes ou de Michael Ventris pour celui de l'écriture crétoise dite Linéaire B montrent que le caractère de langue morte voire inconnue n'a pas toujours constitué un obstacle infranchissable pour le déchiffrement à partir du moment où on disposait d'indices comme la pierre de Rosette trilingue ou l'hypothèse que l'écriture crétoise était en fait du grec syllabique.*
10 *Livres de Nicky Hager « the Secret Power » et de James Banford « the Puzzle Palace ».*
11 *Notamment le Premier ministre néo-zélandais David Lange.*
12 *Seul ce premier rapport est public.*
13 *Pour le responsable du SGR, enquêter sur un système comme Echelon serait illégal en Belgique vu l'absence de législation sur les écoutes de sécurité.*
14 *Réponse à M. Georges Sarre le 24 février 2000.*
15 *Réponse à une question écrite du député Yves Nicolin le 10 janvier 2000.*
16 *Par exemple, dans la réponse à la question écrite de M. Michel PAJON en date du 3 juillet 2000.*
17 *Une enquête préliminaire sert à déterminer si les faits sont suffisamment avérés pour ouvrir une information judiciaire.*
18 *Les messages non déchiffrés ne sont jamais échangés.*
19 *La méthode consiste à remplacer un alphabet en clair par un alphabet crypté en décalant la valeur de chaque lettre (par exemple, A devient C, B devient D, etc.). La clé de chiffrement ou de déchiffrement est alors le décalage de chaque lettre par rapport à sa place normale dans l'alphabet (dans l'exemple : 3).*
20 *Le carré de Vigenère utilise 26 alphabets chiffrés, chacun d'eux étant décalé d'une lettre par rapport au précédent. Son utilisation repose sur un mot ou une expression clé qui permet de savoir à quel alphabet il faut faire référence pour crypter chaque lettre.*
21 *ASCII assigne à chaque lettre de l'alphabet ou à certains symboles un nombre binaire à 7 chiffres.*
22 *Mathématiquement, le nombre d'échanges de clés nécessaires entre « n » individus est « n(n+1)/2 ».*
23 *Dans ce cas, le nombre de clés nécessaires pour « n » intervenants n'est plus que de « 2n ».*
24 *En l'occurrence le produit de ces deux nombres premiers.*
25 *En France, il existe actuellement cinq laboratoires agréés par le SCSSI qui effectuent l'évaluation des systèmes de sécurité.*
26 *ou STOA (scientific and technological option assessment).*
27 *Cf. annexe 3.*
28 *Dont le titre est « The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition ».*
29 *Dont le titre est « The legality of the interception of electronic communications : a concise survey of the principal legal issues and instruments under international, european and national law ».*
30 *Dont le titre est « The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception ».*
31 *Cette résolution a été publiée 22 mois plus tard, au journal officiel des communautés du 4 novembre 1996.*
32 *Les Quinze de l'Union européenne, les partenaires du pacte UKUSA et la Norvège.*