PARLEMENT EUROPÉEN

L' affaire ECHELON

Les travaux du Parlement européen sur le système global d'interception, 1998 - 2002

ÉTUDE

Série sur l'histoire du Parlement européen

EPRS | Service de Recherche du Parlement européen

Auteurs : Franco Piodi et Iolanda Mombelli

Unité Archives historiques

Octobre 2014 – PE 538.877

Archives historiques du Parlement européen
Série sur l'histoire du Parlement européen
Octobre 2014

L'affaire ECHELON

Les travaux du Parlement européen sur le système global d'interception

Étude

EPRS | Service de Recherche du Parlement européen

PARLEMENT EUROPÉEN

Auteurs de l'étude : Franco PIODI et Iolanda MOMBELLI

PARLEMENT EUROPÉEN

DIRECTION GÉNÉRALE DES SERVICES DE RECHERCHE PARLEMENTAIRE

UNITÉ ARCHIVES HISTORIQUES

arch-info@europarl.europa.eu

Couverture :
http://en.fotolia.com/ - Fotolia_49113209 © Maksym Yemelyanov

Luxembourg : Office des Publications de l'Union européenne.

PE 538.877
ISBN: 978-92-823-6001-9
DOI: 10.2861/69522
CAT: QA-02-14-934-FR-N

Imprimé au Luxembourg

Résumé

Au cours de la seconde moitié des années 1990, les médias dévoilèrent l'existence du réseau Echelon. Ce système d'interception des communications privées et économiques, développé et géré par les États signataires du traité UKUSA, se caractérisait alors par sa puissance et par la variété de ses cibles : ce n'étaient plus uniquement les organisations et installations militaires qui étaient surveillées, mais aussi les gouvernements, les organismes internationaux et les entreprises du monde entier.

La présente publication retrace d'abord la découverte de ce réseau, notamment au travers des investigations du STOA, des questions des parlementaires européens, des discussions en séance plénière, de la mise en place d'une commission temporaire et de la prise de position finale du Parlement. Elle rassemble également les déclarations de chercheurs et de journalistes concernant les aspects techniques et les implications juridiques du réseau Echelon. Elle examine enfin les positions des groupes politiques du Parlement européen, de la Commission et du Conseil.

Quinze ans après les faits, *L'affaire Echelon* puise dans les archives du Parlement européen pour décrire et analyser un scandale planétaire, qui marqua l'histoire de l'institution et qui fait aujourd'hui écho aux révélations d'Edward Snowden, de Julian Assange et à bien d'autres affaires d'espionnage à grande échelle.

TABLE DES MATIÈRES

REMARQUES LIMINAIRES

La présente publication des Archives historiques est consacrée à l'affaire Echelon, qui, à cheval sur deux millénaires, a mobilisé la classe politique européenne et passionné l'opinion publique comme peu d'autres initiatives parlementaires. Elle couvre principalement les travaux d'une commission temporaire sur la question, active entre 2000 et 2001, et examine la période allant de 1997 (publication du premier document du STOA sur Echelon) à 2002, année au cours de laquelle, au terme du mandat de la commission temporaire, le Parlement européen a adopté une résolution critiquant le suivi donné par la Commission et le Conseil à sa résolution de l'année précédente.

Le présent ouvrage est fondé presque exclusivement sur des documents du Parlement européen, en grande partie des actes de la commission temporaire Echelon ou des documents, y compris externes, qui lui ont été soumis. Il convient de souligner que les procès-verbaux de la commission sont extrêmement concis et, à quelques exceptions près, ne permettent pas de reconstituer les débats. Par conséquent, les documents présentés en séance ont été majoritairement utilisés.

Du point de vue de l'accessibilité, ces documents peuvent être classés en deux catégories :

- débats et procès-verbaux de l'Assemblée, rapport final de la commission temporaire Echelon (rapport Schmid), questions parlementaires, propositions de résolution et résolutions, c'est-à-dire l'ensemble des documents présentés ou examinés en assemblée plénière, qui sont disponibles dans le Journal officiel de l'Union européenne ou sur le site du Parlement européen : http://www.europarl.europa.eu

- actes et documents de la commission temporaire Echelon et autres documents conservés par les Archives historiques du Parlement européen. Le public peut y avoir accès sur demande au service de documentation, dans la mesure où les documents ne portent pas la mention "Confidentiel", apposée par leur rédacteur, ne se rapportent pas à des réunions à huis clos de la commission Echelon ou ne sont pas considérés comme tels à la date de la demande du document. Une partie de ces documents est également disponible en ligne sur le site du Parlement européen http://www.europarl.europa.eu/comparl/tempcom/echelon/default.htm, où vous trouverez plus d'informations sur la commission.

ABBREVIATIONS

ALE	Alliance libre européenne
CIA	Central Intelligence Agency
COMINT	Communications intelligence
EDD	(Groupe pour l') Europe des démocraties et des différences
ELDR	Libéraux, démocrates et réformateurs européens
GCHQ	Government Communications Headquarters
GUE/NGL	Gauche unitaire européenne/Gauche verte nordique
NSA	National Security Agency
OTAN	Organisation du traité de l'Atlantique Nord
PESC	Politique étrangère et de sécurité commune
PESD	Politique étrangère de sécurité et défense
PPE	Parti populaire européen
PSE	Parti socialiste européen
RDE	Groupe du rassemblement des démocrates européens
STOA	Scientifical and Technological Options Assessment
TDI	(Groupe) technique des députés indépendants
UEN	Union pour l'Europe des nations
UKUSA	United Kingdom-United States of America Agreement

CHAPITRE I

LE SYSTÈME ECHELON DANS LES ÉTUDES DU STOA ET LES PREMIÈRES RÉACTIONS PARLEMENTAIRES

1. Echelon : contexte général

Le nom Echelon désigne un système d'interception des télécommunications construit et géré par les services de renseignements des États-Unis d'Amérique en collaboration avec leurs homologues d'autres puissances occidentales. Il sert à intercepter les communications téléphoniques (conversations et télécopies) et les courriers électroniques d'autres pays, y compris alliés.

En 1996, alors que certaines rumeurs dans la presse avaient déjà dénoncé l'existence de ce système, le STOA[1], sur une proposition du député britannique Glyn Ford, a abordé cette question dans le cadre d'une étude générale, intitulée *An Appraisal of Technologies of Political Control*, dont la publication en 1998 a donné lieu à l'examen de ces rumeurs au niveau politique. Cette étude portait sur le sujet des interceptions en général. Toutefois, deux pages (les pages 19 et 20) dédiées aux réseaux d'interception des communications nationales et internationales révélaient, pour la première fois dans un document de littérature grise relativement officiel, l'existence du système Echelon. Le passage clé est le suivant :

Le système Echelon fait partie du système UKUSA, mais, contrairement à la plupart des systèmes d'espionnage électronique développés pendant la guerre froide, Echelon est principalement conçu pour des cibles non militaires : gouvernements, organisations et entreprises dans presque tous les pays. Le système Echelon opère en interceptant indifféremment de très grandes quantités de communications et en extrayant ensuite les données utiles à l'aide d'outils d'intelligence artificielle comme Memex.[2]

En 1999 est publié un deuxième document, intitulé *Development of surveillance technology and risk of abuse of economic information*, qui approfondit les thèmes indiqués dans son titre, à savoir les technologies de surveillance et leur utilisation à des fins commerciales[3].

Sur la base de ces études, il est possible de reconstituer non seulement la capacité d'Echelon en matière de collecte et d'analyse des communications privées, mais également le cadre institutionnel dans lequel ce système opérait. Ce "cadre institutionnel" désigne les services de renseignements et leurs liens internationaux. L'expression "liens internationaux" doit être comprise dans ce contexte comme un système d'accords entre les services, échappant au contrôle normal que les parlements nationaux ont sur la politique étrangère de leurs États respectifs.

---

[1] ***Scientifical and Technological Options Assessment (STOA)***, un service de la direction générale des recherches du Parlement européen chargé de mener, sous la direction d'un groupe de députés européens, des études sur les aspects techniques et scientifiques des politiques communautaires.

[2] Wright, Steven, *An appraisal of technologies of political control - Interim study*, Working document for the STOA Panel, European Parliament, Directorate General for Research - PE 166.499/Int.St. - Luxembourg, 19 January 1998.

[3] *Development of Surveillance Technology and Risk of Abuse of Economic Information - Appraisal of Technologies of Political Control (Volume 1 to 5)*. Working document for the STOA Panel, European Parliament, Directorate General for Research - PE 168.184 (DG-4-JOIN_ET - 1999).

Les activités de renseignements d'Echelon couvrent la collecte d'informations techniques et secrètes dans les communications étrangères par des individus autres que les destinataires de ces informations, activités désignées par l'abréviation COMINT[4]. Echelon est donc un système de COMINT, mis en place dans le cadre de l'UKUSA, un accord secret[5] entre les systèmes de COMINT britannique et américain ; le Canada, l'Australie et la Nouvelle-Zélande ont par la suite rejoint cet accord. La structure la plus importante des États-Unis pour le COMINT et pour la gestion d'Echelon est l'américaine NSA, à laquelle correspond le GCHQ britannique. Du point de vue quantitatif, le STOA estime que l'accord UKUSA gérait 120 systèmes satellites de collecte d'informations, dont 40 ciblant les satellites occidentaux de communications commerciales.

Au niveau technique, les activités de COMINT d'Echelon, semblent être caractérisées par la capacité de sélectionner, parmi les messages interceptés, ceux qui revêtent de l'importance pour les utilisateurs et doivent dès lors être analysés. Ce tri consiste essentiellement en un traitement automatisé de listes de contrôle, c'est-à-dire des listes de noms de personnes ou d'organisations en rapport avec le message intercepté. Ce traitement automatisé, rendu nécessaire par la quantité énorme de messages interceptés, permet de détecter ceux qui concernent des organisations ou des sujets placés sous contrôle. Toutefois, du moins à la fin des années 1990, lors de la rédaction des documents du STOA, la recherche par mots clés, à savoir la capacité à reconnaître un mot dans une conversation téléphonique, était impossible, contrairement aux informations parues dans la presse ; il était toutefois possible de faire une recherche par sujet de conversation.

Du point de vue de l'utilisation d'Echelon, l'espionnage économique est celui qui retient le plus l'attention, car il concerne également des particuliers et affecte le bon déroulement de la concurrence, en octroyant aux entreprises qui participent à Echelon un avantage concurrentiel injuste et avec lequel il est difficile de rivaliser.

La NSA ne cache pas qu'elle collecte des informations économiques, en se justifiant par le fait que, dans le haut débit, les communications civiles se mêlent aux communications militaires et politiques, mais elle a nié mener une politique prévoyant d'intervenir spécifiquement en réponse aux intérêts d'une entreprise donnée. Toutefois, chaque pays de l'accord UKUSA autorise ses services et ministères à planifier et recevoir des informations économiques, qui ne sont dès lors pas recueillies au hasard, de telle manière qu'une autorité américaine a préconisé l'espionnage industriel en tant qu'élément de protection de la sécurité nationale. Le Royaume-Uni et l'Australie se livrent également à l'espionnage économique.[6]

Le document du STOA de 1999 mentionne quelques cas spécifiques d'espionnage économique dont les informations étaient par la suite communiquées à l'Advocacy Center, un service du Département américain du commerce, et qui permettaient à des sociétés américaines d'en profiter pour l'acquisition de contrats à l'étranger :

- en 1993, l'entreprise PANAVIA a été espionnée concernant des ventes au Moyen-Orient ;

- en 1994, la NSA a intercepté des communications téléphoniques entre Thompson et le Brésil concernant un contrat en vue d'un système de surveillance de la forêt amazonienne, pour lequel l'existence d'actes de corruption était suspectée ; le contrat a finalement été attribué à une entreprise américaine collaborant au système Echelon ;

---

[4] Trente États environ mènent des activités d'interception COMINT : outre les États-Unis et leurs alliés, le principal pays est la Russie, mais la Chine dispose également d'un système puissant. Citons également des membres de l'OTAN, extérieurs à Echelon, qui mènent leurs propres activités autonomes de COMINT, comme la France et l'Allemagne.

[5] L'accord secret a été signé en 1947 a été rendu public en 1999, lorsque le gouvernement australien a confirmé son existence.

[6] STOA, PE 168.184, vol. 2/5, point 5: *Comint and economic intelligence*.

- il en a été de même pour l'interception de communications entre Airbus et ses interlocuteurs saoudiens en 1995 : dans ce cas aussi, la mise au jour d'actes de corruption a été utilisée pour faire attribuer un contrat aux sociétés américaines Boeing et McDonnell Douglas Corp ;

- des sources fiables ont également fait état de pratiques d'espionnage dans le cadre de négociations internationales, en particulier l'interception de communications relatives aux normes d'émissions des véhicules japonais, aux négociations commerciales relatives à l'importation de voitures de luxe japonaises, à la participation de la France aux négociations du GATT depuis 1993 et à la Coopération économique pour l'Asie-Pacifique (APEC).

2. Les premières réactions : les questions parlementaires et la résolution de septembre 1998

Le premier document du STOA soulève l'émoi dans les milieux parlementaires européens et donne lieu, entre 1998 et 1999, à une série de questions, la plupart écrites, mais aussi pour l'heure des questions, toutes adressées à la Commission sauf une au Conseil. En substance, celles-ci anticipent le débat sur la question qui aura lieu en 2000 et 2001. On notera que toutes les questions proviennent de la droite italienne, des Verts et du groupe GUE, à l'exception de deux questions présentées respectivement par un libéral néerlandais et un eurodéputé français du groupe RDE[7].

Les thèmes des questions posées vont de l'existence d'Echelon et des activités d'espionnage des services secrets britanniques à la capacité de la Commission à protéger ses communications confidentielles et les États membres, à la possibilité de permettre aux citoyens d'utiliser des systèmes de chiffrement avancés pour se protéger des activités d'espionnage.

Les réponses de la Commission, toutes évasives et consistant à dire que ces questions ne relèvent pas de ses compétences dans sa prétendue incapacité à agir sur la base d'informations non officielles, montrent le malaise de l'Institution en ce qui concerne la question Echelon.

Quant au Conseil, à la seule question qui lui est posé, il répond laconiquement : *Le Conseil n'a pas connaissance des questions évoquées*.[8]

[7] Questions écrites n° 1039/98 et n° 1040/98 de Nel van Dijk à la Commission : *Écoutes par le MI6 et Echelon*, JO C du 19 novembre 1998, p. 55. Question écrite n° 1306/98 de Cristiana Muscardini et autres députés à la Commission : *Système Echelon et espionnage visant les pays de l'UE*, JO C 402 du 22 décembre 1998, p. 9. Questions écrites n° 1775/98 et n° 1776/98 de Lucio Manisco au Conseil et à la Commission : *Système d'espionnage Echelon*, JO C 13 du 18 janvier 1999, p. 81 et JO C 50 du 22 février 1999, p. 90. Question écrite n° 2329/98 de Nikitas Kaklamanis à la Commission : *Réseau Echelon*, JO C 50 du 22 février 1999, p. 142. Questions écrites de Esko Seppänen, n°1894/98 à la Commission : *Participation de l'Union européenne à l'espionnage électronique*, et n° 2966/98 *Écoutes électroniques illégales*, JO C 142 du 21 mai 1999, p. 3 et p. 63. Question écrite n° 337/99 de Giuseppe Rauti à la Commission : *Système d'espionnage des États-Unis en Europe*, JO C 341 du 29 novembre 1999, p. 94. Question de l'heure des questions n°101 (H-0092/99) d'Ioannis Theonas : *Atteintes à la vie privée*, Débats du Parlement européen 4-533 du 10 février 1999, p. 258. Question de l'heure des questions n° 69 (H-1067/98) de Patricia McKenna : *Sécurité électronique et électromagnétique des institutions de l'UE*, Débats du Parlement européen 4-530 du 16 décembre 1998, p. 238.

[8] Il s'agit de la question écrite n° 1775/98 posée au Conseil par le député Manisco.

La députée néerlandaise Nel van Dijck présente deux questions écrites à la Commission sur les écoutes par le MI6 et Echelon. © Union européenne, 1998

Ce malaise est très probablement lié à la nécessité de ne pas perturber les relations avec le Royaume-Uni, dont l'implication dans le système Echelon ressort clairement des documents du STOA, comme avec les États-Unis, alors que les relations transatlantiques traversent une période particulièrement délicate. On note ce malaise également dans la discussion relative à la première résolution du Parlement européen sur les relations transatlantiques et le système Echelon, du 16 septembre 1998, qui traite, bien qu'incidemment, de cette affaire.[9]

Pendant la séance du 14 septembre, le commissaire Bangemann consacre aux relations transatlantiques et au système Echelon, une déclaration délibérément séparée entre celle initiale sur les relations transatlantiques et celle finale qui met en évidence l'intérêt relatif accordé à la question Echelon par la Commission, qui déclare qu'elle ne peut fonder son action que sur des informations reçues de sources officielles et non sur des sources journalistiques ou une étude. De plus, aucun État membre, aucune entreprise de l'Union

[9] Débats du Parlement européen 4-524 du 14 septembre 1998, pp. 14-24, et Résolution du Parlement européen du 16 septembre 1998, JO C 313 du 12 octobre 1998, p. 98. La résolution est adoptée à un moment où les relations transatlantiques sont perturbées par la loi Helms-Burton, en vertu de laquelle les États-Unis prennent des mesures contre les entreprises non américaines qui entretiennent des relations commerciales avec Cuba.

ou aucun citoyen européen n'a fourni la moindre preuve de l'existence d'Echelon ni du fait que ce système était encore opérationnel.

Si la prudence relative à la question Echelon marque les positions de la Commission et du Conseil, elle ressortira aussi dans la résolution du Parlement qui ne critique pas mais reconnaît le "rôle crucial" de la surveillance électronique *lorsqu'il s'agit de mettre un terme ou d'empêcher les activités des terroristes, des trafiquants de drogue et du crime organisé*[10] ; il est toutefois "essentiel" que les technologies de surveillance soient utilisées dans le cadre de systèmes de contrôle démocratique. Le Parlement européen demande un débat ouvert sur ces technologies, tant au niveau national qu'au niveau de l'Union européenne, ainsi que l'adoption d'un code de conduite destiné à garantir la réparation d'erreurs ou d'abus et, avec une référence spécifique à Echelon, *l'adoption de mesures de protection des informations économiques et d'un cryptage efficace*.

3. Année 2000 : premiers signes de reprise du débat

Après la résolution de 1998 et les questions du premier trimestre de l'année suivante, la campagne électorale pour les élections européennes de 1999 et la période de démarrage ultérieure de la nouvelle législature éclipsent le débat sur Echelon, lequel est rouvert, encore plus vif qu'auparavant, au début de l'année 2000. Ce débat est relancé par l'audition de la commission des libertés civiles sur l'Union européenne et la protection des données, au cours de laquelle est présenté le deuxième document du STOA consacré à Echelon, dont l'existence a été entre-temps confirmée par des sources américaines.[11] L'audition de la commission des libertés civiles se conclut par une déclaration de son président Graham Watson, qui contient deux points principaux : les entreprises européennes victimes d'espionnage industriel dans le cadre d'Echelon sont invitées à se faire connaître, étant donné que le deuxième document du STOA ne contient pas suffisamment d'informations à ce sujet et, en ce qui concerne en particulier les travaux parlementaires, il appartient désormais aux groupes politiques de décider du suivi à donner à l'affaire Echelon.[12]

La première décision est un débat sur la question, qui aura lieu le 30 mars 2000, mais, presque simultanément à l'audition, on constate des prises de position de dirigeants politiques importants. Ainsi, la présidente du Parlement européen, Nicole Fontaine, déclare : *On peut être légitimement scandalisé que cet espionnage, qui a lieu depuis plusieurs années, n'ait pas donné lieu à des protestations officielles. Pour l'Union européenne, les intérêts en jeu sont essentiels. D'une part, il semble établi qu'il y a eu violation des droits fondamentaux de ses citoyens, d'autre part l'espionnage économique a pu avoir des conséquences désastreuses, par exemple sur l'emploi*.[13]

---

[10] Résolution du Parlement européen du 16 septembre 1998, JO C 313 du 12 octobre 1998, p. 99.

[11] Compte rendu de l'audition *L'Union européenne et la protection des données*, les 22 et 23 février 2000, Bruxelles, PE5 AP PV/LIBE.1999 LIBE-20000222-2 0005 et *Hearing in Parliament on 22 and 23 February*, Agence Europe, 5 février 2000. Pour le document STOA, voir p. 9 du présent document.

[12] *EP/Privacy - Echelon case creates a stir at the hearin*g, *Plenary debate on 30 March 2000*, Agence Europe, 24 février 2000.

[13] *UE/Affaire Echelon - Après l'audition de PE, Mme Fontaine s'interroge sur les suites,* Agence Europe, 25 février 2000.

CHAPITRE II
VERS LA CRÉATION DE LA COMMISSION ECHELON

1. Le débat en plénière du 30 mars 2000

Venons-en à présent au débat du 30 mars 2000 sur les déclarations du Conseil et de la Commission sur l'existence du système d'intelligence artificielle permettant aux États-Unis d'Amérique d'intercepter et de surveiller toutes les communications téléphoniques et électroniques de l'Union européenne (Echelon), qui se terminera par quatre propositions de résolution. Trois d'entre elles, demandant la création d'une commission d'enquête, auront une issue négative.[14]

Le président en exercice du Conseil Justice et Affaires intérieures, Fernando Gomes, fait une déclaration qui sera jugée insatisfaisante par presque tous les députés européens qui sont intervenus par la suite, car elle ne contient aucune prise de position sur les responsabilités spécifiques dans l'affaire Echelon, dont l'existence est qualifiée de "possible" par Gomes. Toutefois, le président du Conseil s'est prononcé clairement sur le problème général de l'interception : *Le Conseil ne peut accepter la création ou l'existence d'un système d'interception des télécommunications qui ne respecte pas les règles de droit des États membres* [...].

La déclaration du commissaire Liikanen ne soulève pas non plus l'enthousiasme des députés. L'intervention ne mentionne même pas le système Echelon, mais rend compte des réponses fournies dans une lettre par le Royaume-Uni aux demandes d'éclaircissements de la Commission. Le pays y déclare que les services secrets britanniques travaillent dans les limites d'un cadre juridique fixé par le parlement du Royaume-Uni qui précise explicitement les fins pour lesquelles l'interception peut être autorisée, qu'il existe une commission parlementaire spéciale de surveillance et que la commission des droits de l'homme a considéré que le système prévu par la législation britannique est conforme à la Convention européenne de sauvegarde des droits de l'homme.

Le commissaire Liikanen informe également que la Commission a reçu une lettre du département d'État américain déclarant que *les services secrets des États-Unis n'exercent pas d'activités d'espionnage industriel et que le gouvernement et les services secrets des États-Unis n'acceptent pas de missions pour le compte d'entreprises privées* [...].

Le débat qui suit porte essentiellement sur les prolongements à donner à l'affaire Echelon.

Pour le PPE, l'eurodéputée allemande Klamt, qui considère comme claires les déclarations du Conseil et de la Commission, se concentre sur les propositions visant à créer une commission d'enquête, ce qu'elle juge inutile. Elle est surtout préoccupée par l'espionnage industriel et propose une approche internationale avec la mise à l'ordre du jour de ce thème à la Conférence mondial du commerce.

Le socialiste allemand Schulz évalue de manière négative les déclarations des deux autres institutions, mais, s'agissant de la question de la commission d'enquête, il se montre plus

[14] Débats du Parlement européen du 30 mars 2000. Les trois propositions en faveur de la création d'une commission d'enquête ont été déposées par les membres italiens du groupe UEN (B5-0287/2000), plusieurs membres du groupe GUE/NGL (B5-0294/2000) et d'autres membres du groupe Verts/ALE (B5-0302/2000) ; la quatrième proposition (B5-0290/2000) a été présentée par des membres du groupe TDI. Une cinquième proposition, qui n'a jamais été présentée officiellement (B5-0398/2000), a été approuvée par la commission des libertés civiles le 11 avril 2000, voir procès-verbal PE5 AP PV/LIBE.1999 LIBE-20000411 0010.

prudent car *la base juridique qui justifie une telle commission doit également être explicitée de manière irréprochable si l'on veut qu'elle puisse réussir*.

Au nom du Groupe ELDR, le député néerlandais Wiebenga se déclare lui aussi insatisfait des déclarations de MM. Gomes et Liikanen et *estime qu'il faut prendre cette affaire au sérieux. Car si elle est vraie, les droits du citoyen peuvent aussi être violés*.

Le président du groupe des Verts, M. Lannoye, n'est pas non plus satisfait par les déclarations et il ne regrette pas la proposition de son groupe de créer une commission d'enquête, car *nous savons que ce système existe, mais nous ne savons pas exactement comment il fonctionne* ; *il y a de fortes raisons de croire [que] le Royaume-Uni collabore à ce système.*

Discours "embarras[sés]" et "emberlificotés" c'est ainsi que M. Wurtz, président du groupe GUE/NGL, décrit les déclarations du Conseil et de la Commission. Concernant la création d'une commission d'enquête, il déclare : *Que cela plaise ou non, le dossier 'Echelon' est désormais ouvert et le restera*.

Le député Berthu, du groupe UEN, se dit *stupéfai[t] par l'exposé du Conseil* et s'associe, au nom de son groupe, à la proposition de création d'une commission d'enquête.

M. Belder, du groupe EDD, insiste moins sur l'existence de techniques d'interception que sur la question de la légitimité de leur utilisation : *Le profit économique ne peut pas la justifier. Le droit des personnes à la vie privée ne peut pas être violé de la sorte.*

Le député Martinez, du groupe TDI, intervient de manière passionnée et oppose les idéaux de la concurrence et de la compétitivité à la pratique de l'espionnage industriel, le principe de solidarité au sein de la Communauté à la solidarité transatlantique, dont a fait preuve le Royaume-Uni.

Une voix se lève pour défendre le Royaume-Uni : le socialiste britannique Evans apprécie les déclarations du Conseil et de la Commission et relève :

Comme M. Liikanen l'a déclaré, tout ce qui est fait au Royaume-Uni est conforme à un cadre juridique approprié. Tout fait l'objet d'un examen parlementaire minutieux par la Chambre des Communes. Nous avons des contrôles très étroits, un contrôle indépendant et un contrôle réalisé par le secrétaire d'État avec le plein consentement du gouvernement du Royaume-Uni.

2. Commission d'enquête ou commission temporaire ?

La mise aux voix des propositions de résolution présentées lors du débat du 30 mars, qui a été reportée à la session de mai 2000, n'aura pas lieu, mais la question fondamentale, à savoir la création d'une commission d'enquête sur l'affaire Echelon, sera à l'ordre du jour de trois réunions de la Conférence des présidents les 13 avril, 11 mai et 15 juin 2000.

Le président du Parlement reçoit en effet deux demandes de création d'une commission sur Echelon. La première demande vise la constitution d'une commission d'enquête et provient de M. Paul Lannoye, président du groupe Verts/ALE, qui a recueilli 170 signatures.[15]

[15] Lettre du 27 mars 2000 adressée à Nicole Fontaine, présidente du Parlement européen, PE5 OD PV/CPRG CPRG-20000413 0070. Le minimum de signatures requises par l'article 151 du Règlement du Parlement européen est d'un quart des membres, c'est-à-dire 157 en 2000.

Les motivations sont liées à l'article 151 du Règlement du Parlement européen, qui prévoit que les commissions d'enquête examinent les infractions au droit communautaire, et, à cette fin, les dispositions communautaires susceptibles d'être enfreintes par Echelon sont citées. Les bases juridiques sont l'article 6 du traité UE, qui consacre le respect des droits fondamentaux, dont le respect de la vie privée, et l'article 286 du traité CE, qui prévoit le contrôle par des autorités indépendantes de l'application des règles communautaires relatives au traitement des données à caractère personnel[16] ; sur la base de cette disposition, la proposition de création d'une commission d'enquête indique que les institutions communautaires sont tenues de prendre les mesures qui s'imposent pour garantir la sécurité des services qu'elles fournissent. Un autre point qui justifie la création de la commission demandée est la violation de l'article 81 du traité, qui interdit les pratiques qui ont pour objet de fausser le jeu de la concurrence, comme cela semble être le cas pour l'affaire Echelon.

La deuxième demande a été introduite par le président du groupe socialiste, l'espagnol Barón Crespo[17], qui propose une commission temporaire[18] en en précisant le mandat :

- *des initiatives politiques pour une coopération plus loyale entre les États membres* ;

- *des initiatives pour empêcher à des pays tiers toute forme d'interception sur le territoire de l'Union allant au-delà des exigences de la lutte commune au crime organisé ; des actions nécessaires afin que la protection de la vie privée soit garantie* ;

- *des mesures législatives pour la mise à jour et l'harmonisation des dispositions en matière de protection de données personnelles* ;

- *des initiatives appropriées pour l'adoption d'outils et de technologies (câblage, cryptage…) aptes à contrecarrer les interceptions en provenance de pays tiers*.

En d'autres termes, les demandeurs d'une commission d'enquête estiment que le système Echelon constitue une violation du droit communautaire et le règlement prévoit l'instrument spécifique requis pour examiner cette question.

Par contre, le motif pour la création d'une commission temporaire est lié aux limites que la commission d'enquête aurait par rapport à son mandat : elle peut examiner des violations du droit communautaire dans le cadre du traité CE (article 193) et, dès lors, une commission d'enquête ne peut se saisir que des matières qui y sont visées. Sont donc exclus les domaines qui relèvent du titre V (PESC) et du titre VI (Coopération policière et judiciaire en matière pénale) du traité UE.

Cependant, il n'est pas illogique de supposer que le souci de ne pas nuire aux relations avec le Royaume-Uni, qui aurait été inévitablement accusé si une commission d'enquête avait été créée, a joué un rôle dans le choix des grands groupes, qui concentrent la quasi-totalité des membres britanniques du Parlement.

Enfin, il peut être utile d'examiner les principaux pouvoirs d'une commission d'enquête, établis sur la base d'une décision commune des trois institutions politiques[19]. L'article 3 de

[16] Il s'agit en particulier de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.95, pp. 31-50), et de la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO L 24 du 30.1.97, pp. 1- 8).

[17] Lettre du 13 avril 2000 adressée à Nicole Fontaine, présidente du Parlement européen, PE5 OD PV/CPRG CPRG-20000615 0070.

[18] Régie par l'article 150, paragraphe 2, du Règlement du Parlement européen, juin 1999, libellé comme suit: *[…] le Parlement peut, à tout moment, constituer des commissions temporaires dont les attributions, la composition et le mandat sont fixés en même temps que la décision de leur constitution.*

cette décision régit la comparution devant la commission de fonctionnaires des institutions et des États membres, autorisés à comparaître par l'institution ou par l'État membre *à moins que des motifs de secret ou de sécurité publique ou nationale ne s'y opposent, du fait d'une législation nationale ou communautaire*. Ces mêmes restrictions s'appliquent à l'obligation des institutions et des États membres de fournir à la commission d'enquête les documents nécessaires à ses travaux.

Compte tenu de la nature particulière de l'affaire Echelon, il est hautement probable qu'une commission d'enquête se serait vu opposer largement les restrictions susmentionnées et on peut dès lors présumer que le choix d'une commission temporaire n'avait pas pour finalité d'éviter l'application de la décision de 1995, mais obéissait à des raisons d'opportunité politique comme supposé ci-dessus. D'un autre côté, tandis que la commission d'enquête, malgré ces restrictions, peut examiner les documents nécessaires à ses travaux, une commission temporaire ne peut utiliser que des documents appartenant au domaine public.

Dès sa réunion du 13 avril, la Conférence des présidents avait rejeté la proposition de création d'une commission d'enquête et approuvé la constitution d'une commission temporaire, dont la création sera décidée le 15 juin. Les deux décisions de la Conférence, soit le rejet de la commission d'enquête et la création d'une commission temporaire, seront ratifiées par l'Assemblée le 5 juillet 2000.

3. Le mandat et les membres de la commission temporaire

Sur la base de la décision adoptée[20], la commission Echelon a été instituée avec le mandat suivant :

- vérifier l'existence du système d'interception des communications connu sous le nom d'Echelon [...] *;*

- 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.

---

[19] Décision du Parlement européen, du Conseil et de la Commission du 19 avril 1995 portant sur les modalités d'exercice du droit d'enquête du Parlement européen (95/167/CE) JO L 113 du 19 mai 1995, pp. 1-4. Aux fins du présent document, nous avons consulté l'annexe VIII du Règlement du Parlement européen, juin 1999.

[20] Décision du Parlement européen portant constitution d'une commission temporaire sur le système d'interception Echelon (B5-0593/2000), JO C 121 du 24 avril 2001, p. 131.

M. Carlos Coelho, président de la commission temporaire sur le système d'interception Echelon 2000-2001. © Union européenne, 2011

Ce mandat a une durée de douze mois, la durée maximale prévue par l'article 150 du Règlement du Parlement européen. La commission se compose des 36 députés suivants[21] :

14 membres du groupe PPE-DE[22] : Banotti, von Boetticher, Cederschiöld, Coelho, Deprez, Dimitrakopoulos, Hernández Mollar, Klamt, Hugues Martin, Oostlander, Palacio Vallelersundi, Pirker, Van Velzen, Zappalà, *Buttiglione*, *Cornillet*, *Gawronski*, *Giannakou-Koutsikou*, *Nassauer*, *Posselt*, *Johan Van Hecke* ;

11 membres du groupe PSE[23] : Berger, Robert Evans, Karamanou, Catherine Lalumière, Lund, Erika Mann, Medina Ortega, Paasilinna, Gerhard Schmid, Vattimo, Wiersma, *Andersson*, *Caudron*, *Ford*, *Gebhardt*, *Marinho*, *Paciotti*, *Swiebel*, *Swoboda*, *Terrón i Cusí*, *Thielemans*, *Titley* ;

3 membres du groupe ELDR : Di Pietro, Flesch, Plooij-van Gorsel, *Andreasen*, *Thors*, *Dybkjær* ;

3 membres du groupe Verts/ALE[24] : Ceyhun, MacCormick, McKenna, *Boumediene-Thiery*, *Ilka Schröder*, *Lambert* ;

2 membres du groupe GUE/NGL : Di Lello Finuoli, Krivine, *Frahm*, *Papayannakis* ;

1 membre du groupe UEN : Berthu[25], *Nobilia* ;

---

[21] Nous indiquons en italique les membres suppléants, qui ne comptent pas parmi les 36 membres.

[22] Outre les remplacements indiqués dans les notes qui suivent, une liste ultérieure des membres de la commission comporte quelques modifications concernant les membres suppléants du groupe PPE-DE, au sujet desquelles aucune communication spécifique n'a été retrouvée dans les archives du Parlement européen.
M. Nassauer ne figure plus sur la liste et les députés Bradbourn, Jean-Pierre, Matikainen-Kallström et Oomen-Ruijten font leur apparition. Dans la décision portant constitution de la commission, le groupe PPE-DE n'avait pas utilisé toutes ses possibilités de membres suppléants.

[23] Ce chiffre passera à 12 membres avec l'arrivée de M. Ceyhun.

[24] Le groupe Verts/ALE ne comptera plus que deux membres après le départ de M. Ceyhun pour le groupe socialiste.

1 membre du groupe TDI : Turco, *Frank Vanhecke* ;

1 membre du groupe EDD : Belder, *Okking*.

Le 6 juillet 2000, lors de sa réunion constitutive, la commission temporaire sur le système d'interception Echelon élit comme président Carlos Coelho, et comme vice-présidents, Elly Plooij-van Gorsel, Neil MacCormick et Giuseppe Di Lello Finuoli. Gerhard Schmid est nommé rapporteur.

Mme Elly Plooij-van Gorsel, vice-présidente de la commission temporaire sur le système d'interception Echelon 2000-2001. © Union européenne, 2003

4. La méthode et le programme de travail

Les questions de la méthode et du programme sont au centre des réunions des 5, 11 et 12 septembre 2000. Nous disposons des procès-verbaux, des notes à la présidence, des projets de calendrier et de programme de travail, d'un document de travail du rapporteur qui consiste en un résumé du programme de travail accompagné d'une synthèse des méthodes approuvées lors de la réunion.

Dans un passage du rapport, le président affirme que la "crédibilité" de la commission sera la ressource fondamentale pour acquérir les informations nécessaires. La crédibilité réside essentiellement dans la capacité de la commission dans son ensemble et de chacun de ses membres à traiter sous le sceau du secret les documents confidentiels qu'ils recevront, de même que les points soulevés lors des réunions à huis clos, qui seront décidées par le Bureau sur proposition du président[26]. La commission garantira aux personnes extérieures au Parlement qui lui présenteront des documents confidentiels que ceux-ci ne seront divulgués aux membres ou à des tiers que dans les limites définies au moment de la transmission desdits documents. Cette garantie va au-delà de ce qui est prévu à l'annexe VII du Règlement du Parlement[27], à laquelle le procès-verbal fait explicitement référence.

---

[25] Après avoir quitté le groupe UEN (30 janvier 2001), M. Berthu sera remplacé par M. Marchiani, dont le nom ne figure pas sur la liste de membres ultérieure. Il n'a été retrouvé aucune trace de ce remplacement dans les archives du Parlement européen.

[26] Cette compétence spécifique du Bureau a fait l'objet d'une décision de la commission, probablement prise par consensus, étant donné que le procès-verbal ne mentionne nulle mise aux voix à ce sujet.

[27] Procédure à appliquer pour l'examen des documents confidentiels transmis au Parlement européen.

C'est dans ce contexte qu'il faut placer le programme de travail, lequel, selon la structure adoptée par le rapporteur, se compose de neuf points[28]:

a) Ce que nous savons avec certitude sur le système Echelon,

b) Discussion dans d'autres parlements et au niveau des gouvernements,

c) Activités des agences de renseignement,

d) Les possibilités d'interception des systèmes de communication et leur infrastructure,

e) Chiffrement,

f) Espionnage économique,

g) Les cibles de l'espionnage et leurs mesures de protection,

h) Système juridique et vie privée,

i) Débat sur les recommandations et proposition.

Le niveau de détail du document de travail n° 1 contraste avec l'avant-projet de programme de travail. Ceci laisse penser que la commission s'est livrée à une discussion beaucoup plus approfondie que ce qui ressort du procès-verbal.

[28] Note récapitulative de la réunion et projet de programme de travail de la commission, PE5 AP PV/ECHE.2000 ECHE-20000905 0050.

CHAPITRE III

LES CONSULTATIONS DE LA COMMISSION

1. La contribution des experts : les questions sur le système

La commission Echelon organise plusieurs auditions d'experts du secteur dont l'expertise se fonde sur leur expérience en tant que consultants pour des organismes publics et des entreprises privées, de chercheurs et de journalistes ayant enquêté sur Echelon. Tous ont basé leurs recherches sur des sources ouvertes et publiques, lesquelles, si elles sont suivies régulièrement et correctement analysées, fournissent néanmoins des informations utiles.

Trois experts méritent une attention particulière, pour l'apport qu'ils avaient déjà donné à la phase de rédaction du document STOA.

Le premier est Duncan Campbell, le journaliste qui a dévoilé l'affaire Echelon et a participé à la rédaction des documents du STOA. Celui-ci a mis l'accent sur le rôle d'Echelon dans l'espionnage économique, surtout commercial, en mettant ces activités en rapport avec celles du département du commerce des États-Unis et en soulignant les préjudices occasionnés à l'économie européenne. Echelon n'intercepte pas toutes les données, mais se concentre sur des priorités définies et sur les demandes de ses "clients". En particulier sont illustrés de nombreux cas de réussite de l'Advocacy Center du gouvernement américain, qui a pour mission de soutenir les entreprises américaines dans leurs relations commerciales avec l'étranger en s'appuyant apparemment sur le système Echelon.[29]

Le deuxième, James Bamford[30] a présenté un compte rendu détaillé du système d'espionnage américain. La NSA est une agence d'espionnage plus importante que la CIA. Elle remplit une fonction de collecte de renseignements et, selon M. Bamford, elle représente une menace plus grave pour la vie privée des individus que pour les entreprises. Quant aux renseignements sur les entreprises non américaines que la NSA cherche à obtenir, ils concerneraient essentiellement la violation des sanctions économiques imposées à certains pays et il déclare qu'il n'a aucune preuve de transmission d'informations de la NSA aux entreprises américaines.

Le troisième, Nicky Hager, chercheur et journaliste d'investigation néo-zélandais, a analysé la situation des interceptions dans le Pacifique Sud, les relations entre les États Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande, surtout du point de vue de l'espionnage commercial. Il souligne que, selon ses sources, son pays exerce l'activité de "monitoring" en tant que membre de l'alliance UKASA avec la conscience que s'il ne joue pas son rôle, il pourrait être lentement exclu de cet accord. Il conclut que, toujours selon les informations qu'il a collectées et par analogie, la situation en Europe est comparable à celle dans le Pacifique Sud.[31]

---

[29] M. Campbell a produit plusieurs documents qui ont été inclus dans le dossier de la réunion des 22 et 23 janvier 2001, PE5 AP PV/ECHE.2000 ECHE-20010122.

[30] Journaliste d'investigation américain, auteur de deux livres, l'un paru en 1982, consacré à la NSA, et l'autre, *Body of Secret*, publié après son audition du 23 avril 2001. Au sujet de son audition, nous disposons du procès-verbal de la commission temporaire Echelon, PE5 AP PV/ECHE.2000 ECHE-20010423 0010, plus détaillé que les autres documents, et d'un aide-mémoire du secrétariat de la commission, voir PE5 AP PV/ECHE.2000 ECHE-20010423 0025.

[31] Nicky Hager a écrit plusieurs livres, dont *Secret Power: New Zealand's Role in the International Spy Network*, Nelson 1996, cité dans le document du STOA de 1998. Il a été auditionné par la commission Echelon le

Le procès-verbal de la réunion du 12 octobre 2000, au cours de laquelle un premier groupe d'experts a été entendu, est quelque peu succinct, mais un autre document[32] fournit un cadre global sur le rôle d'Echelon dans l'espionnage économique au bénéfice d'entreprises américaines et, plus généralement, sur le système et les méthodes que les États-Unis emploient pour exercer un contrôle sur les informations économiques, contrôle qui est parfois motivé par la lutte contre la criminalité et la corruption internationales.

Un autre document d'une source externe qu'il convient de mentionner est le *Rapport complémentaire d'activités 1999* du Comité permanent de contrôle des services de renseignement belges[33], lequel ne consiste pas en une étude des activités des services belges, mais examine les documents produits sur Echelon, principalement ceux du STOA, et place le système américain d'interception dans le contexte technologique et juridique approprié. Selon le document, *Echelon peut capter la totalité du trafic satellitaire à destination de l'Europe* et cette *capacité de déchiffrement est gigantesque, mais tout à fait minimisée par les services américains*. Par ailleurs, *toute technologie américaine (software et hardware) licitement exportée vers l'Europe est considérée comme intrinsèquement et volontairement sujette à une surveillance aisée, à distance et discrète par les services américains.*

Toujours selon le document, une surveillance basée sur un dictionnaire de mots clés est possible sur le courrier électronique non chiffré et aussi sur le trafic téléfax, s'il utilise les satellites ; par contre ce n'est pas possible sur les communications téléphoniques satellitaires (environ 1% des communications téléphoniques internationales) *mais est possible la reconnaissance d'un locuteur particulier sur base de son empreinte vocale*.

En janvier 2001, la commission entend plusieurs journalistes et chercheurs indépendants, qui ont examiné le cas Echelon et, plus généralement, la question de l'espionnage électronique. En particulier, deux chercheurs danois présentent les capacités d'interception du Danemark et les relations de ce pays avec certains pays de l'accord UKUSA[34].

Le document *Espionnage industriel – intelligence économique et stratégique* suit une perspective différente, celle du point de vue de l'utilisateur de l'espionnage économique, dont la philosophie est exposée dans une citation d'un ancien directeur de la CIA, William Webster : *Nos alliés politiques et militaires sont aussi des rivaux économiques et les capacités d'un rival économique à créer, capturer ou contrôler des marchés dans l'avenir ont des implications en matière de sécurité pour les États-Unis.* Le document montre qu'au Japon et en Chine existent aussi des services qui pratiquent l'espionnage industriel.[35]

Un autre document, *L'Europe face au défi de l'intelligence stratégique*, dénonce le retard en matière de renseignement stratégique dont souffre l'Europe et critique la Commission,

---

23 avril 2001 et le compte-rendu de son intervention est disponible en anglais, PE5 AP PV/ECHE.2000 ECHE-20010423 0026.

[32] Von Coester, S., *Système Echelon – éléments de réflexion – sources ouvertes*. PE5 AP PV/ECHE.2000 ECHE-20001012 0080. Son auteur est le directeur du cabinet de conseil stratégique Salamandre (France).

[33] *Rapport complémentaire sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau Echelon d'interception des communications*, http://www.crid.be/pdf/public/4226.pdf.

[34] Procès-verbal de la commission temporaire Echelon des 22 et 23 janvier 2001, PE5 AP PV/ECHE.2000 ECHE-20010122 0010.

[35] Document présenté lors de la réunion de la commission du 6 mars 2001 par M. La Fragette, de l'entreprise française Circé, qui fournit des conseils dans le domaine de l'espionnage industriel, PE5 AP PV/ECHE.2000 ECHE-20010305 0075.

qu'il juge imperméable à toute discussion sur l'utilisation de l'information dans le domaine géoéconomique[36].

2. La contribution des experts externes : les questions juridiques

Une illustration complète et détaillée des aspects juridiques est fournie dans le document *Echelon et Europe*, présenté à la commission par Dimitri Yernault lors de l'audition des experts du 22 mars 2001. Le document examine le caractère illicite d'Echelon du point de vue de différents systèmes juridiques.[37]

Du point de vue du **droit international**, le point de départ est la notion, généralement admise, de l'extension territoriale de la souveraineté d'un État : une compétence juridique extraterritoriale ne peut se réaliser en dehors d'un État qu'avec le consentement (appelé "exequatur") de l'État territorialement souverain sur le lieu d'exécution. Les interceptions menées dans le cadre du système Echelon, qui visaient des personnes et des entités situées en dehors de l'État dans lequel se trouvaient les installations, doivent dès lors être jugées contraires au droit international.

Du point de vue de la **responsabilité**, si un État ne peut être tenu pour responsable du comportement d'organismes internationaux, même si ceux-ci opèrent sur son territoire, il a néanmoins l'obligation de contrôler ce qui se passe sur son territoire et de prendre les précautions nécessaires pour éviter les violations du droit international. Cette obligation de contrôle devient importante dans le contexte d'Echelon, car elle concerne la responsabilité des pays qui ont autorisé les États-Unis à se servir de bases situées sur leur territoire.[38]

Du point de vue de la **Convention européenne des droits de l'homme** est important de citer son article 8 paragraphe 1 (Droit au respect de la vie privée et familiale) :

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, où le terme "correspondance" doit être compris au sens large de *gamme complète des services de télécommunications*[39]. En vertu de l'article 8, paragraphe 2, une autorité publique ne peut procéder à une interception que si cela est prévu par une loi, et uniquement aux fins indiquées dans ce paragraphe. Il s'ensuit que l'interception doit respecter les conditions de légalité et de nécessité.

Le principe de légalité a été défini par la Cour européenne des droits de l'homme en ce sens que l'interception est prévue par une loi facilement accessible et prévisible[40]. Les lois

---

[36] Document présenté par M. Harbulot, directeur de l'École de guerre économique, réunion de la commission temporaire du 5 mars 2001, PE5 AP PV/ECHE.2000 ECHE-20010305 0060.

[37] Communication aux membres d'un document de M. Dimitri Yernault intitulé *Echelon et Europe* - PE 300.134, PE5 AP PV/ECHE.2000 ECHE-20010322 0082. Ce document reproduit un article homonyme publié dans le *Journal des Tribunaux – Droit européen* (Bruxelles), octobre 2000, pp. 187-196. Le procès-verbal de la réunion du 22 mars 2001, PE5 AP PV/ECHE.2000 ECHE-20010322 0010, présente de manière résumée les déclarations de M. Yersault.

[38] Le document mentionne le cas spécifique de l'Allemagne, qui aurait permis d'utiliser sa base de Bad Aibling sans participer aux activités qui y ont été menées.

[39] Conseil de l'Europe – Recommandation nº R (95) 4 F du 7 février 1995 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques.

[40] Dans la jurisprudence citée, la notion d'"accessibilité" semble plus large que la notion habituelle de "publication". La prévisibilité signifie que le texte de loi est suffisamment clair pour faire comprendre dans quelles circonstances et dans quelles conditions l'autorité publique est autorisée à procéder à des interceptions ; les instructions et les pratiques administratives doivent également être suffisamment connues des personnes concernées. Leander c. Suède, Requête n° 9248/81, Arrêt de la Cour européenne des droits de l'homme du 26 mars 1987.

qui régissent le système Echelon ne sont pas facilement accessibles, ni aux États-Unis, ni au Royaume-Uni, où les accords relatifs à l'utilisation de la base de Menwith Hill sont également inaccessibles, y compris pour les membres du Parlement.

La notion de nécessité implique surtout que l'ingérence dans la vie privée doive correspondre à un besoin social impérieux et qu'elle soit, en particulier, proportionnée au but légitime poursuivi. Sur la base de cette notion, la Cour européenne des droits de l'homme affirme que *les États ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée.*[41]

Un système tel qu'Echelon qui opère des interceptions exploratoires et généralisées ne répond manifestement pas au principe de nécessité et le document en question rappelle que, hors du cadre de la Convention européenne, le Comité des droits de l'homme des Nations unies insiste également sur le fait que les interceptions doivent être autorisées au cas par cas.

Après avoir replacé, sur le fond, le système Echelon dans le contexte de la Convention européenne des droits de l'homme, à laquelle les États-Unis ne font pas partie, le document *Echelon et l'Europe* examine si la Convention peut s'appliquer à Echelon. Cette question est abordée du point de vue de l'applicabilité de la Convention aux activités étatiques menées dans le cadre des relations internationales et, à cet égard, à la lumière de la jurisprudence, le document y répond par l'affirmative, que ce soit sur la base de la théorie de l'organe, qui engage la responsabilité des États pour des actes émanant de leurs organes et déployant leurs effets en dehors de leur territoire[42], ou sur la base de l'obligation qui incombe aux États de contrôler les actes commis sur leur territoire ou depuis celui-ci, obligation que nous avons déjà mentionnée.[43]

Un autre aspect abordé est la recevabilité d'un recours contre Echelon devant la Cour européenne des droits de l'homme. Si la jurisprudence exclut les recours présentés par des citoyens non concernés directement, certains arrêts ont admis les recours déposés par des victimes potentielles, considérées comme telles par la simple existence de mesures de surveillance secrètes ou d'une loi qui permet une telle surveillance, sans qu'il soit nécessaire de prouver que lesdites mesures s'appliquent concrètement à la victime.[44]

3. La position de la Commission et du Conseil

L'exécutif s'est exprimé lors des auditions de la commission par l'intermédiaire d'Antonio Vitorino, commissaire à la justice et aux affaires intérieures, et d'Erkki Liikanen, commissaire aux entreprises et à la société de l'information, entendus les 11 et

---

[41] Klass et autres c. Allemagne, Requête n° 5029/71, Arrêt de la Cour européenne des droits de l'homme du 6 septembre 1978.

[42] Drozd et Janousek c. France et Espagne, Requête n° 12747/87, Arrêt de la Cour européenne des droits de l'homme du 26 juin 1992.

[43] Il s'ensuit que la Convention prime sur les autres accords internationaux conclus par un état et dès lors, en ce qui concerne Echelon, sur l'accord UKUSA.

[44] Klass et autres c. Allemagne, Requête n° 5029/71, Arrêt de la Cour européenne des droits de l'homme du 6 septembre 1978, et Rotaru c. Roumanie, Requête n° 28341/95, Arrêt du 4 mai 2000. Le document susmentionné est le plus détaillé et le plus complet des documents juridiques qui ont été présentés lors de la réunion du 22 mars 2001. Citons d'autres documents également importants : *Cyber-rights vs Cyber-crimes* (PE 300.135), présenté par l'association britannique Cyber-Rights & Cyber-Liberties; *Protection de la vie privée et droits de l'homme*, présenté par M. Nataf, avocat, et M. Coste, expert en sécurité informatique, *The interception of communications and unauthorised access to information stored on computer systems in the light of the European Convention on Human Rights*, présenté par M. Dossow, fonctionnaire du Conseil de l'Europe.

12 septembre 2000[45], et de Christopher Patten, commissaire aux relations extérieures, entendu le 3 avril 2001.

Comme lors des déclarations de la Commission au cours du débat du 30 mars, les commissaires Vitorino et Liikanen traitent de questions générales qui relèvent de leurs compétences respectives dans le domaine de la sécurité des télécommunications et non directement d'Echelon. M. Vitorino se concentre sur la protection de la vie privée dans le cadre de la directive européenne 95/46/CE relative à la protection des données. De son côté, le commissaire Liikanen se concentre sur le chiffrement, qui doit être fiable et fournir un niveau élevé de protection, et sur les outils cryptographiques qui doivent rester entre les mains des institutions pour garantir une lutte efficace contre la criminalité.

Parallèlement, le commissaire Patten déclare que, bien que les activités des services de renseignements américains ne soient pas à l'ordre du jour du Nouvel Agenda transatlantique, la question Echelon sera abordée lors d'une rencontre des ministres de la justice et des affaires intérieures. S'agissant de la question plus spécifique de la sécurité de l'information, M. Patten informe qu'après l'approbation du règlement sur la sécurité du Conseil, l'exécutif est en train d'approuver son propre règlement qui mettra en place un système détaillé de traitement des diverses formes d'informations classifiées de l'UE et qui donnera à la Commission un niveau de sécurité approprié à son rôle dans le cadre de la PESC et de la PESD.[46] À la suite des déclarations des commissaires, ce sont surtout les réponses de M. Patten qui provoquent le mécontentement d'au moins une partie des membres de la commission.

M. Christopher Patten, commissaire aux relations extérieures entendu par la commission Echelon le 3 avril 2001. © Union européenne, 1999

La position du Conseil sera présentée à la commission par Hervé Masurel, président du Conseil en exercice, le 28 novembre 2000[47]. Le Conseil estime que les interceptions sont une arme importante dans la lutte contre la criminalité, mais que leur utilisation pour obtenir des avantages commerciaux est inacceptable. S'agissant de la question spécifique d'Echelon, si son existence est désormais admise, il n'existe aucune preuve de son éventuelle utilisation à des fins commerciales ou en violation des droits des citoyens

[45] M. Vitorino répond par une plaisanterie à une question sur l'existence d'Echelon : *Je crois en Dieu et à Echelon, mais je n'ai jamais rencontré ni l'un ni l'autre. PE/Espionnage - La commission temporaire du Parlement européen sur le système Echelon a entamé ses travaux*, Agence Europe, 13 septembre 2000.

[46] En plus que le PV de la réunion, deux autres documents sont disponibles pour l'intervention du Commissaire Patten : Contribution du commissaire Chris Patten pour la commission temporaire Echelon du Parlement européen, PE5 AP PV/ECHE.2000 ECHE-20010403 0026, et Note présentant la retranscription des questions à M. Patten et ses réponses - réunion sur Echelon du 3 avril 2001 - Strasbourg, PE5 AP PV/ECHE.2000 ECHE-20010403 0028.

[47] Retranscription des déclarations d'Hervé Masurel et Arthur Paecht, PE5 AP PV/ECHE.2000 ECHE-20001128 0020.

européens. Il insiste en particulier sur l'importance du chiffrement et de la mise en œuvre d'une architecture de sécurité des réseaux informatiques.

Pour le Conseil intervient aussi Brian Crowe, directeur général des relations extérieures[48], qui attache une grande importance à la distinction entre les compétences des États et celles du Conseil : le renseignement relève de la compétence des premiers. Il souligne également que le Conseil enregistre d'importants progrès dans la réalisation d'un système sécurisé de télécommunications et négocie avec l'OTAN un accord sur la question.

La présidence suédoise est entendue le 29 mai 2001, en la personne de l'ambassadeur Lund, qui se contente d'exposer les mesures prises par le Conseil sur les questions relevant de la compétence de l'Union et cite en particulier la "Sphère de sécurité" sur la protection des données à caractère personnel[49].

Les déclarations du Conseil, et notamment l'intervention de M. Masurel, ne satisfont pas au moins deux membres de la commission[50].

4. La contribution des parlements nationaux

Outre la déclaration du Conseil, la réunion de la commission du 28 novembre 2000 est consacrée à l'audition des parlements nationaux, et plus précisément à celle des organes chargés de contrôler les services de renseignements nationaux ou des députés qui ont examiné ou examinent le cas Echelon. Seuls quatre parlements ont envoyé des représentants : le Parlement irlandais, le Sénat belge, le Nationalrat autrichien et l'Assemblée nationale française. Les documents de la présidence indiquent que la Finlande, la Norvège et les Pays-Bas ont déclaré qu'ils n'étaient pas en mesure d'envoyer des représentants, mais aucune information ne peut être obtenue en ce qui concerne l'absence des représentants du Luxembourg et de l'Espagne, dont la présence était mentionnée dans l'ordre du jour avec l'indication "À confirmer" ; enfin, le procès-verbal de la réunion du 22 janvier 2001 nous apprend que le Danemark a refusé d'envoyer un représentant. Aucune information n'est disponible sur la participation des autres parlements nationaux.[51]

Le procès-verbal ne fournit aucun élément utile sur les déclarations de trois des quatre représentants, tandis que l'intervention du représentant de l'Assemblée nationale française et rapporteur sur Echelon, le député Arthur Paecht est largement détaillée. M. Paecht s'est montré acerbe et particulièrement ironique au sujet de ses rencontres avec les autorités américaines. Il a formulé des hypothèses personnelles quant aux raisons

[48] M. Crowe a été entendu le 23 avril 2001. Ses déclarations sont consignées dans le procès-verbal de la commission, PE5 AP PV/ECHE.2000 ECHE-20010423 0010, et dans un aide-mémoire du secrétariat, Compte rendu du discours et de l'échange de vues avec M. Crowe, PE5 AP PV/ECHE.2000 ECHE-20010423 0027.

[49] Les principes de la Sphère de sécurité sont des principes de confidentialité des données à caractère personnel adoptés par le gouvernement des États-Unis le 21 juillet 2000. La décision de la Commission du 26 juillet 2000 sur cette question (JO L 215 du 25.8.2000, p. 7) fait référence à ces principes. Procès-verbal de la commission temporaire Echelon du 29 mai 2001, PE5 AP PV/ECHE.2000 ECHE-20010529 0010.

[50] Procès-verbal (à huis clos) de la commission temporaire Echelon du 28 novembre 2000, PE5 AP PV/ECHE.2000 ECHE-20001128 0010.

[51] Le dossier disponible aux Archives historiques comprend les documents suivants : Documentation relative à la législation des services de contrôle des renseignements en Allemagne, PE5 AP RP/ECHE.2000 A5-0264/2001 0110, Documentation sur la législation en Allemagne : Le contrôle parlementaire des services de renseignements, PE5 AP RP/ECHE.2000 A5-0264/2001 0120, Documentation relative à la législation des services de contrôle des renseignements en Autriche, PE5 AP RP/ECHE.2000 A5-0264/2001 0140, et Tableau synoptique des services de renseignements et des organes de contrôle parlementaire des États membres (projet), PE5 AP PV/ECHE.2000 ECHE-20001128 0030.

de la soudaine attention portée à l'affaire Echelon, alors que les documents à ce sujet étaient déjà disponibles sur Internet. Il pointe l'aspect crucial du problème quand il déclare qu'il n'existe aucune preuve de l'utilisation d'Echelon à des fins d'espionnage industriel, mais que cela n'a aucune importance parce que *techniquement c'est effectivement possible et dès lors que c'est possible [...] ce qui m'importe c'est qu'on se protège et que ce n'est pas la France ou l'Allemagne ou les Pays Bas qui vont se protéger isolément, c'est bien un problème de l'Union européenne [...]*[52].

[52] Retranscription des déclarations d'Hervé Masurel et Arthur Paecht, du 28 novembre 2000, p. 4, PE5 AP PV/ECHE.2000 ECHE-20001128 0020.

Système global électronique de surveillance : Echelon écoute tout le trafic d'e-mail, téléphone, fax et télex qui est transmis globalement par satellite
Graphique : Archives historiques © Union européenne 2014

CHAPITRE IV

LES TRAVAUX DE LA COMMISSION ET LE RAPPORT FINAL

1. Les missions à Paris, à Londres et à Washington

Parallèlement aux consultations, des délégations de la commission se sont rendues en mission à Paris, Londres et Washington, avec divers degrés de réussite.

La mission à **Paris** du 18 janvier 2001 consiste principalement en une réunion entre le président de la commission, M. Coelho, le rapporteur, M. Schmid, le secrétaire général de la Défense nationale, Jean-Claude Mallet, et cinq de ses collaborateurs. La délégation de la commission a également été reçue au Quai d'Orsay et au ministère de la Défense.

Le secrétaire général de la Défense nationale présente son point de vue sur les informations disponibles à l'égard d'Echelon et sur les possibles enjeux en la matière. Il évoque aussi les thèmes du chiffrement et de la coopération dans le domaine du renseignement dans le cadre de l'identité européenne de sécurité et de défense.[53]

Au ministère de la Défense, le conseiller du ministre, M. Perraudau, présente les structures que la France met en place pour protéger les ministères et les entreprises des interceptions et fait part de la nécessité de mutualiser les sources d'information des États membres sur certains domaines stratégiques spécifiques.

La visite à **Londres**, effectuée du 24 au 26 janvier 2001, consiste en plusieurs réunions, dont une avec le président de la commission du renseignement et de la sécurité de la Chambre des Communes, M. King, qui expose les fonctions de cette commission : celle-ci a accès à tous les documents secrets qui ne concernent pas des opérations en cours et à toute base des services de renseignements. Un échange de vues sur l'interception des communications satellite a aussi eu lieu.

Le secrétaire d'État à l'intérieur, M. Straw, rencontré par la suite, met l'accent sur la convention relative à l'entraide judiciaire et sur la loi britannique en matière d'interception, qu'il compare à celle de certains pays européens ; il explique par ailleurs ses fonctions en ce qui concerne l'autorisation des interceptions.[54]

Pour la mission à **Washington** du 6 au 11 mai 2001, les membres de la délégation ont dû faire face au refus de les rencontrer de la part des nombreuses agences de renseignements et des départements d'État et du Commerce.

En conclusion, la mission se résume à une réunion avec la commission permanente du Congrès sur le renseignement, réunion que M. Coelho jugera très utile et constructive, à une réunion avec James Woolsey, ancien directeur de la CIA, et à des réunions avec des organismes privés. L'appréciation globale de l'issue de la mission et les considérations politiques relatives à l'attitude des autorités américaines sont clairement indiquées dans

[53] Les documents disponibles à ce sujet sont inclus dans le dossier de la réunion de la commission temporaire des 22-23 janvier 2001, PE5 AP PV/ECHE.2000 ECHE-20010122, lequel comprend un aide-mémoire en anglais, qui a été largement utilisé pour la rédaction de notre texte, une lettre de remerciement du président Coelho au secrétaire général de la Défense nationale, la liste des membres des deux délégations.

[54] Les documents disponibles à ce sujet sont inclus dans le dossier de la réunion de la commission temporaire des 5-6 fevrier 2001, PE5 AP PV/ECHE.2000 ECHE-20010205, lequel comprend la note à la Présidence, plusieurs contributions d'experts et une note du responsable du secrétariat, M. Lowe, relative à une de ses visites préliminaires.

le procès-verbal de la réunion du 15 mai 2001, au cours de laquelle le président rend compte à la commission en déclarant qu'il *déplore que les rencontres prévues avec des représentants du département d'État, de l'Advocacy Center du ministère du Commerce, de la CIA et de la NSA aient été annulées à la dernière minute, sans explication satisfaisante,* tout en précisant que *la délégation n'a jamais eu pour objectif de recueillir des informations supplémentaires et déplore que les services et les agences qui se sont désistés se soient privés de l'occasion d'expliciter leur rôle dans cette affaire en refusant tout débat.* [55]

MM. Carlos Coelho et Gerhard Schmid (avec M. David Lowe à gauche) à la conférence de presse du 16 mai 2001, suite à la visite de la délégation de la commission Echelon aux États-Unis. © Union européenne, 2001

Le traitement réservé à la délégation suscite des réactions. Tout d'abord, la présidente du Parlement européen, M[me] Fontaine, exprime ses regrets devant le refus des principales administrations américaines de rencontrer la délégation, empêchant ainsi la commission Echelon de mener à bien ses travaux. Néanmoins, la présidente remercie tout de même les membres du Congrès pour leur disponibilité au dialogue. Une position similaire sera prise par le Parlement quelques jours plus tard avec la résolution sur l'état du dialogue transatlantique.[56]

[55] Communiqué de M. Coelho lors de la visite à Washington, PE5 AP PV/ECHE.2000 ECHE-20010515 0040 et Procès-verbal de la commission temporaire Echelon du 6 mai 2001, PE5 AP PV/ECHE.2000 ECHE-20010515 0010.

[56] Communiqué de la présidence du Parlement européen concernant le refus de certaines autorités américaines de recevoir les délégués à Washington, PE5 AP PV/ECHE.2000 ECHE-20010515 0050, et Résolution sur le dialogue transatlantique (résolution commune B5-0345/2001) du 17 mai 2001, JO C 34E du 7 février 2002, pp. 255-359. Les références à cette question au cours du débat du 16 mai sont rares.

2. Le rapport Schmid : les caractéristiques d'Echelon[57]

La commission adopte l'imposant rapport Schmid et le projet de résolution qui l'accompagne le 3 juillet 2001, avec 27 voix pour, 5 contre et 2 abstentions ; les votes contre et les abstentions sont motivés dans quatre avis minoritaires.

Le rapport présente un inventaire complet des informations obtenues sur Echelon (même les contacts confidentiels du rapporteur), des activités d'interception menées à l'extérieur de ce système, des implications juridiques et concrètes de l'espionnage économique et des technologies utilisées, et il aborde la question du chiffrement, lequel est considéré comme la principale défense possible contre l'interception.

Le point de départ du rapport est l'observation selon laquelle un système d'interception mondial, appelé Echelon, existe. Une grande partie du rapport, le chapitre V, intitulé *Preuves par indices de l'existence d'au moins un système d'interception mondial*, est consacrée à l'examen des sources qui permettent d'affirmer l'existence d'Echelon et celle de l'accord UKUSA. Le chapitre VI, intitulé *Peut-il exister d'autres systèmes d'interception mondiaux?*, répond à cette question par l'affirmative et se concentre en particulier sur les cas de la France, de l'Allemagne, de la Russie et de la Chine.

La principale caractéristique d'Echelon est sa portée mondiale, rendue possible par la collaboration entre plusieurs États dans le cadre de l'accord UKUSA. À cette portée mondiale il convient d'ajouter les capacités techniques, grâce auxquelles Echelon peut intercepter presque toutes les formes de télécommunications, même si chacune d'elles implique différentes manières d'y avoir accès et des difficultés de degrés différents.

Si les interceptions des **communications par satellite** ne présentent pas trop de difficultés pour un réseau qui dispose de centres d'interception dans les régions appropriées de la planète, l'interception des **transmissions hertziennes** dépend de la portée des ondes radio à intercepter : pour les *ondes de sol*, c'est-à-dire les ondes qui suivent la courbe de la surface terrestre, leur portée sera limitée et, dès lors, la possibilité de les intercepter également ; pour les *ondes d'espace ou indirectes*, c'est-à-dire les ondes envoyées dans l'ionosphère, qui les renvoie vers le sol, leur portée est plus importante et il est donc plus aisé de les intercepter. Pour les **transmissions par câble**, qui couvrent tous les types de télécommunications, il est nécessaire de disposer d'un accès physique au point d'arrivée du câble et l'interception est donc toujours possible pour l'État sur le territoire duquel le câble transite, tandis qu'un État étranger n'y aura accès qu'avec la collaboration de l'État de transit ou par des moyens illégaux. D'autres problèmes sont encore ceux liés à l'interception des **transmissions par câble sous-marins**, possibles au moyen de sous-marins, avec évidemment des coûts très élevés et que la dernière génération de fibres optiques rend impossibles.

Il s'ensuit que les pays UKUSA disposent d'excellents moyens pour intercepter les transmissions par satellite, de peu de moyens pour intercepter les transmissions hertziennes et de moyens très limités pour intercepter les transmissions par câble, moyens qui, en Europe, se limitent de fait au Royaume-Uni.

Étant donné que les interceptions internationales, contrairement aux interceptions nationales menées à des fins judiciaires, ne sont pas ciblées, il convient d'ajouter, aux limites en matière d'accessibilité des diverses formes de télécommunications, la difficulté de sélectionner les communications pertinentes parmi l'énorme quantité de

[57] Rapport du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON), PE5 AP RP/ECHE.2000 A5-0264/2001 0010, p. 26. Les paragraphes qui suivent présentent le rapport en se concentrant sur les aspects les plus importants politiquement.

communications interceptées. Au moment du rapport il était possible de repérer une voix donnée, si le système était formé pour la reconnaitre. Par contre, la reconnaissance automatique de mots prononcés par une voix quelconque était encore impossible avec une précision suffisante.

3. Le rapport Schmid : les aspects juridiques[58]

Une autre caractéristique d'Echelon est que ce système opère en dehors de tout cadre juridique. À cet égard, il convient de citer directement le rapport :

Les risques que pourrait présenter, pour la sphère privée et les milieux économiques, un système du type ECHELON ne résultent pas uniquement du très grand potentiel de ce système de surveillance, mais procèdent bien davantage du fait qu'il fonctionne dans un espace qui échappe, pour l'essentiel, à toute règle juridique. Un système d'interception des communications internationales ne vise pas la plupart du temps les habitants du pays qui l'exploite. De par son statut d'étranger, la personne dont les messages sont interceptés ne dispose ainsi d'aucune protection juridique intérieure. Aussi, l'individu est-il entièrement à la merci du système. Dans ce domaine, le contrôle parlementaire est également insuffisant, dès lors que les électeurs, qui partent du principe qu'ils ne sont pas concernés et que 'seules' sont concernées des personnes à l'étranger, ne manifestent pas un intérêt particulier pour cette question, et que pour les élus, ce qui compte avant tout, ce sont les intérêts de leurs électeurs. Aussi ne faut-il pas s'étonner que les auditions sur les activités de la NSA, qui ont eu lieu au sein du Congrès américain, aient porté uniquement sur la question de savoir si des citoyens américains étaient également victimes de ce système [...] .

L'absence de cadre juridique régissant Echelon ne signifie pas qu'il soit impossible d'examiner son statut juridique. Le rapport cherche un instrument pour sanctionner un système d'espionnage et le trouve à l'article 10 du traité CE, appliqué comme suit :

Si un État membre prêtait assistance à un système d'interception, destiné entre autres à également espionner les entreprises, en permettant d'utiliser à cet effet ses propres services de renseignement ou en mettant son territoire à la disposition de services de renseignement étrangers, alors, il pourrait très bien y avoir violation du droit communautaire. En effet, aux termes de l'article 10 du traité CE, les États membres ont un devoir de loyauté générale et doivent en particulier s'abstenir de toutes mesures susceptibles de mettre en péril la réalisation des buts du [...] *traité*.

Et de conclure :

En résumé, il est possible de dire qu'en principe, dans la situation juridique actuelle, un système de renseignement du type Echelon ne saurait être contraire au droit de l'Union, dès lors qu'il ne présente aucun rapport avec des éléments du droit de l'Union justifiant son incompatibilité. Il en va toutefois uniquement ainsi tant que le système est utilisé exclusivement aux fins de garantir la sûreté de l'État au sens large. S'il est par contre détourné de ses objectifs pour espionner des entreprises étrangères, il y a bien infraction au droit communautaire. Et si un État membre participait à une activité de ce type, il violerait le droit communautaire.

4. Le rapport Schmid : la protection des citoyens contre les activités d'interception[59]

La protection des citoyens contre les interceptions menées par des organismes publics relève de la compétence exclusive des États et est soumise à des règles différentes selon que l'interception a lieu dans le cadre d'une enquête policière ou judiciaire ou est

[58] Rapport A5-0264/2001, point 1.6, 7.3 et 7.4.
[59] Rapport A5-0264/2001, point 9.3 et 9.4.

effectuée par les services de renseignement, lesquels, dans les régimes démocratiques, exercent leurs activités uniquement à des fins prévues par la loi.

En ce qui concerne les interceptions menées dans le cadre d'enquêtes policières ou judiciaires, les garanties sont assez homogènes dans l'ensemble des États membres et elles prévoient normalement une autorisation préalable de l'autorité judiciaire. S'agissant des interceptions menées par les services de renseignements, qui ne concernent généralement pas des utilisateurs spécifiques mais des groupes considérés comme potentiellement dangereux, les garanties sont assez différentes d'un État à l'autre.

Un outil indispensable pour la protection des citoyens contre les interceptions menées par les services de renseignements est le contrôle exercé sur ceux-ci, qui est diversement mis en œuvre dans les États membres et qui, la plupart du temps, relève de la responsabilité de commissions spéciales. Les conclusions tirées dans le rapport sont peu satisfaisantes pour les citoyens européens car les pouvoirs des services de renseignements présentent des différences notables. Les activités et les pouvoirs des organes de contrôle et *leurs effets défavorables concernent avant tout les ressortissants des autres États, puisque les activités des services de renseignements à l'étranger concernent par définition l'extérieur du pays. Le citoyen est relativement sans défense face aux systèmes étrangers. Le besoin de protection est donc plus grand encore dans ce domaine.*

5. Le rapport Schmid : la protection contre l'espionnage économique[60]

L'expression "espionnage économique" désigne les activités d'espionnage menées par un service de renseignement étatique envers des entreprises, généralement étrangères. Cette notion est différente de l'"espionnage de concurrence" ou encore de l'"espionnage industriel", lequel intervient entre entreprises, normalement concurrentes, mais également dans le domaine des relations commerciales.

À de nombreux égards, le rapport ne suit pas cette distinction et traite globalement de l'espionnage exercé sur les entreprises. Les données sur les dommages causés par l'espionnage consistent en des évaluations controversées et hétérogènes, dont la seule conclusion que l'on puisse tirer est la certitude que les dommages sont élevés.

Le rapport se concentre sur l'espionnage économique, tel que défini ci-dessus, afin d'identifier les États qui mènent de telles activités, sur la base du niveau de leur technologie. Les pays les plus avancés dans ce domaine auront pour objectif de mieux définir leurs politiques économiques ou industrielles ou d'acquérir des informations utiles à leurs entreprises qui participent à des marchés dans d'autres États. Les pays les moins avancés viseront l'acquisition à faible coût de savoir-faire.

L'une des formes majeures de l'espionnage économique, et qui relève du mandat de la commission Echelon, est l'intrusion dans les réseaux informatiques ou le vol de données sur des supports de stockage électroniques. Les risques sont élevés car, en dehors des grandes organisations publiques et privées, la connaissance de ces risques est faible et, dès lors, rares sont les précautions, même simples, qui sont prises.

Le rapport examine ensuite la perception du risque dans diverses situations, en particulier dans les institutions européennes. La réponse qu'il apporte est la propagation du chiffrement en tant qu'instrument d'autoprotection et analyse la question de la limitation légale du chiffrement prévue dans certains États. Le rapport adopte une position contraire à ces limitations, qui peuvent entraver le développement du commerce sur l'internet et des services de banque électronique.

[60] Rapport A5-0264/2001, point 10.2, 10.5.2, 10.11.

6. Les points saillants du rapport

Le rapport Schmid peut être résumé comme suit :

- un système d'interception mondial, sans doute appelé Echelon, existe réellement et est géré sur la base d'un accord secret (UKUSA) conclu entre cinq pays : les États-Unis (avec le rôle de meneur), le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande ; ce système utilise également des bases dans d'autres États, comme la base de Bad Aibling en Allemagne ;

- ce système n'est pas en mesure, pour des raisons techniques, de permettre l'interception de toutes les communications, pas même de la majorité d'entre elles et il ne peut analyser qu'une quantité réduite de communications ;

- ce système a été effectivement utilisé pour intercepter les télécommunications d'entreprises européennes, au motif de la lutte contre la corruption internationale, et il existe donc un risque que les informations ainsi recueillies soient utilisées pour fournir des avantages aux entreprises américaines ;

- d'autres États possèdent des systèmes d'interception analogues.[61]

M. Gerhard Schmid, rapporteur au fond du Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (Document A5-0264/2001), pendant la réunion de la commission le 12 octobre 2000. À gauche : Reino Paasilinna, membre de la commission temporaire. © Union européenne, 2000

Le rapport est accompagné de 44 recommandations portant sur divers sujets. Celles-ci sont presque toutes reprises dans la proposition de résolution et ensuite dans la résolution. Parmi les recommandations qui n'ont pas été retenues, la plus importante est

[61] Ces quatre points sont une synthèse des conclusions. Rapport A5-0264/2001, point 13.1.

la n° 16 qui, donnant logiquement suite au principe de responsabilité des États membres en vertu de l'article 10 du traité tel qu'interprété par le rapport en référence à l'espionnage économique, invite *les autorités du Royaume-Uni* [...] *à faire la lumière sur leur rôle dans l'alliance UKUSA étant donné que sont établies l'existence d'un système de type Echelon et son utilisation aux fins de collecte de renseignements économiques*. Il s'agit du seul point du rapport qui rappelle, quoique prudemment, le Royaume-Uni à ses responsabilités.[62]

Le rapport est également accompagné de quatre avis exprimés par autant de groupes parlementaires minoritaires au sein de la commission : le groupe GUE/NGL, les Verts/ALE, l'UEN et le groupe TDI. Leur contenu est repris dans les interventions faites lors du débat du 5 septembre 2001.

7. L'affaire Perkins

Pour compléter l'exposition des travaux de la commission Echelon, il semble approprié de mentionner un épisode qui, tout en ne trouvant pas écho dans le rapport, a suscité l'émoi au sein de la commission et dans la presse.

Lors d'une audition d'experts dans le domaine du chiffrement, la commission a entendu Desmond Perkins, le chef de l'unité chargée du chiffrement des communications de la Commission, lequel a déclaré : *J'ai toujours eu de très bons contacts avec la National Security Agency à Washington. Elle vérifie régulièrement nos systèmes (de cryptage) pour voir s'ils sont bien verrouillés et s'ils sont correctement utilisés.*[63]

Cette déclaration provoque une réaction du rapporteur, Gerhard Schmid qui demande à savoir ce qu'on entend par contrôle et vérification par la NSA.

Après une première réponse évasive, M. Perkins déclare: *Parce que j'ai de la famille qui y travaille. C'est aussi simple que cela. Ne l'oubliez pas, et je suis sûr que vous tous ici dans cette salle vous le savez, les Américains lisent tout, peu importe ce qui se passe ici, grâce à tous leurs satellites en réseau* [...]. *La NSA est une organisation gigantesque, elle paie des milliers d'employés juste pour écouter en permanence et lire en permanence.*

Les déclarations de M. Perkins donnent lieu à l'envoi d'une lettre du rapporteur Schmid, dans laquelle celui-ci demande au commissaire Patten des explications sur les relations de la Commission avec la NSA[64]. Pour sa part, M. Perkins sent qu'il est nécessaire de clarifier ses déclarations auprès de son directeur général avec une note quant à sa déclaration selon laquelle les Américains lisent tout. Il y précise que par "lire" il voulait dire simplement que *les Américains interceptent tout type de trafic. Cela ne veut en aucun cas dire qu'ils peuvent nécessairement déchiffrer tout ce qu'ils interceptent* et qu'il ne savait pas *s'ils sont capables de déchiffrer le trafic chiffré de la délégation de la Commission à Washington,* mais selon son expérience c'était improbable.[65]

---

[62] La récommandation n° 21 qui suit, reprise dans la résolution, invite le Royaume-Uni et l'Allemagne à subordonner au respect des droits des citoyens l'autorisation d'interception, au moyen de bases sur leur territoire, de communications par les États-Unis.

[63] Contribution de Desmond Perkins sur le système de chiffrement de la Commission, PE5 AP PV/ECHE.2000 ECHE-20010205 0100.

[64] Lettre du 7 février 2001, Correspondance relative à une contribution lors de la réunion des 5 et 6 février 2001 et qui a soulevée certains malentendus, PE5 AP PV/ECHE.2000 ECHE-20010305 0080, p. 4.

[65] D. Perkins, Note à M. Lagras du 8 février 2001, Correspondance relative à une contribution lors de la réunion des 5 et 6 février 2001 et qui a soulevée certains malentendus, PE5 AP PV/ECHE.2000 ECHE-20010305 0080, p. 2.

En réponse à la lettre de M. Schmid, le commissaire Patten lui transmet, sans commentaires, la note de M. Perkins et l'incident est qualifié de malentendu dans une déclaration du porte-parole de la Commission.[66]

Cependant, la note de M. Perkins et la déclaration du porte-parole ne concluent pas cette affaire car deux fonctionnaires de l'exécutif interviendront lors de la réunion suivante de la commission, afin de fournir des éclaircissements sur les déclarations de M. Perkins[67]. Le procès-verbal de la réunion du 6 mars 2001, dont cette partie se déroule à huis clos, consigne ainsi leurs explications : *M. Briet déclare qu'il assume la responsabilité de M. Perkins, que la Commission est disposée à garantir l'accès aux communications[68] et que l'idée que la NSA veut vérifier les communications de la Commission est absurde ; à son avis, il n'y a pas eu de contacts entre la Commission et la NSA ; il ajoute que tant M. Perkins que d'autres fonctionnaires ont fait objet de surveillance. Il affirme qu'il est vrai qu'il existe la possibilité que nous soyons interceptés et que la Commission doit améliorer ses systèmes de sécurités.*

Si elle a trouvé une conclusion au sein de la commission[69], l'affaire Perkins a eu des répercussions extérieures : les Verts appellent à un débat en plénière car cela dépasse le mandat politique de la commission temporaire et doit être traité dans l'hémicycle, la Commission devant faire une déclaration sur l'accès éventuel de la NSA au système cryptographique de l'exécutif[70] et lors de la séance de l'Assemblée du 12 mars 2001, le groupe présente sa proposition, à laquelle adhère le groupe GUE/NGL. Diffèrente est la position de M. Swoboda qui s'oppose à cette proposition car il estime, tout en soulignant la gravité des déclarations de M. Perkins, qu'il appartient à la commission Echelon, éventuellement avec des pouvoirs élargis, de faire la lumière à ce sujet. La proposition est dès lors rejetée.[71]

---

[66] *Eu/Spying - European Commsission denies Americans are testing EU encryption system*, Agence Europe, 2 mars 2001.

[67] La feuille de présence pour la réunion des 5 et 6 mars 2001 révèle la présence de deux fonctionnaires de la Commission, cités dans le procès-verbal à propos de l'affaire Perkins : M. Briet, directeur adjoint de la direction générale des relations extérieures et donc supérieur hiérarchique de M. Perkins, et M. De Baenst, directeur du protocole et de la sécurité, PE5 AP PV/ECHE.2000 ECHE-20010305 0010.

[68] Sur ce point, le procès-verbal n'est pas précis et cette phrase se prête à des interprétations équivoques: à qui la Commission garantit-elle l'accès aux communications ?

[69] Lors d'une conférence de presse, en réponse à une question spécifique, le rapporteur Schmid fait sienne la position de M. Briet selon laquelle il n'existe aucun document écrit sur l'intervention de la NSA décrite par M. Perkins. *Ep/Echelon - M. Schmid a fait le point sur les travaux de la commission temporaire Echelon,* Agence Europe, 8 mars 2001.

[70] *Pe/Espionnage - M. Lannoye veut un débat en plénière*, Agence Europe, 3 mars 2001.

[71] Débats du Parlement européen du 12 mars 2001, Ordre des travaux.

MM. Carlos Coelho et Gerhard Schmid à la conférence de presse du 11 juillet 2001. © Union européenne, 2001

CHAPITRE V
LA RÉSOLUTION SUR ECHELON ET LES SUITES QUI Y SERONT DONNÉES

1. Le débat en plénière

Le 5 septembre 2001, le rapport Schmid est discuté par l'Assemblée au cours d'un débat serein[72], mais lors duquel apparaissent des positions opposées. Une large majorité des parlementaires s'affirme cependant en faveur de la résolution proposée.

Le président, M. Coelho, résume ainsi les travaux de la commission : *Echelon existe bel et bien, sous cette dénomination ou une autre. Le Parlement européen ne doit avoir aucun doute à ce sujet.* Il souligne que *le système comporte un risque sérieux de mauvaise utilisation, un risque commercial, mais aussi un risque pour les libertés des citoyens et que l'Europe et les États-Unis doivent coopérer loyalement [...] au nom de leurs indiscutables valeurs communes.* Il insiste aussi sur *la nécessité de renforcer la convention européenne des droits de l'homme en ce qui concerne le respect de la protection de la vie privée, la nécessité du contrôle parlementaire et juridictionnel sur les activités des services secrets, la nécessité de la généralisation des pratiques de défense comme l'utilisation de la cryptographie et des signatures numériques, la nécessité pour les institutions européennes, elles-mêmes, de donner l'exemple de l'utilisation de ces technologies.*

Pour sa part, le rapporteur Schmid saisit le sens politique des différentes opinions exprimées au sein de l'Assemblée, il pose le problème de la réponse à donner à l'opinion publique européenne surtout vis-à-vis de la méfiance envers les Américains :

[...] *les gens croient les États-Unis capables d'une telle chose. Le problème politique est une méfiance très profonde, qui est ici de plus en plus évidente. Mais c'est le monde entier qui doit s'en méfier !*

Le rapporteur socialiste est soutenu par le groupe PPE-DE en la personne de M. von Boetticher qui remercie *le rapporteur et son équipe pour ne pas avoir succombé aux tentatives des Verts, mais aussi de la gauche de cette Assemblée, de rédiger un roman de conspiration*. Il considère le rapport sérieux et objectif même si les conclusions, qui exploitent cependant toutes les possibilités juridiques disponibles, ne paraissent pas aller assez loin pour certains.

M. Wiersma, du groupe PSE, met l'accent sur ce que serait une relation appropriée entre services de renseignements et citoyens, en insistant sur l'importance d'avoir *des règles de protection de la vie privée de tous les citoyens européens de tous les pays de l'Union européenne* [...].

Le rapporteur reçoit également le soutien plein et entier du groupe ELDR, pour lequel M^me^ Flesch déclare *illusoire et vain de proposer la suppression des services secrets. Ils existent et continueront à exister. Il convient donc de tirer des conclusions politiques et de rechercher des solutions* [...].

L'avis du groupe des Verts/ALE est diamétralement opposé et M^me^ McKenna demande s'il convient de maintenir leur existence et formule la critique fondamentale de son groupe politique au rapport : *il se concentre principalement sur la menace posée par l'espionnage industriel. Cependant, le véritable enjeu, c'est que personne ne peut plus communiquer en tout confiance.*

[72] Débats du Parlement européen du 5 septembre 2001.

M. Di Lello Finuolin, du groupe GUE/NGL, est sur la même longueur d'onde et souligne qu'Echelon *en raison de son potentiel technique,* [...] *rend vain le rapport de proportionnalité qui, au sens justement de l'article 8 de la convention européenne des droits de l'homme, doit exister entre l'ingérence dans la vie privée et les intérêts à protéger par le biais l'interception.*

M. Marchiani, du groupe UEN, est lui aussi opposé au rapport, mais pour d'autres raisons, dont la principale est que la *majorité anglo-saxonne de cette Assemblée a fait passer la solidarité atlantiste avant la solidarité européenne*.

M. Turco, quant à lui, critique *cette gestion des travaux [...] nécessaire non pour protéger la sécurité européenne, mais pour cacher la responsabilité des États membres*. Selon Turco, le rapport affirme qu'Echelon existe et que le Royaume-Uni participe au système, mais on ne les condamne pas ouvertement parce que l'Allemagne intercepte déjà et les Pays-Bas s'apprêtent à le faire.

M. Belder, du groupe EDD, exprime son soutien au rapport, mais insiste sur un amendement à la proposition de résolution qu'il a déposé, visant *à protéger la communication des interceptions sur lesquelles aucun contrôle n'est exercé*.

2. La résolution

La proposition de résolution est approuvée[73], avec seulement deux amendements, le jour même du débat avec 367 voix pour, 159 contre et 34 abstentions : le vote des membres de chaque groupe n'est cependant pas homogène, à l'exception de ceux des groupes GUE/NGL et UEN, qui votent tous contre.

En substance, la résolution reprend les recommandations de la commission temporaire. Certains points concernent les traités internationaux à conclure ou à modifier et, à cet égard, est particulièrement importante l'invitation à signer une convention entre l'Union européenne et les États-Unis établissant le respect mutuel des dispositions de protection de la vie privée et de confidentialité des communications des entreprises applicables à leurs propres citoyens et entreprises.

Les États membres sont invités à adapter leur législation sur les services de renseignements à la Convention européenne des droits de l'homme en assurant les garanties appropriées non seulement pour leurs propres citoyens, mais également pour ceux de pays tiers, sur la base d'un code de conduite commun, tandis qu'un code analogue devrait être négocié avec les États-Unis. Ils sont également invités *à mettre en commun leurs moyens d'interception des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement, de la lutte contre le terrorisme, la prolifération nucléaire ou le trafic international de stupéfiants, dans le respect des dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises, sous le contrôle du Parlement européen, du Conseil et de la Commission*.

Si tous les États membres sont invités à éviter une utilisation abusive des services de renseignements à des fins économiques, s'agissant en particulier de la participation du Royaume-Uni et de l'Allemagne au système Echelon, ces deux pays sont invités *à subordonner l'autorisation d'interception, sur leur territoire, de communications par les services de renseignements des États-Unis à la condition que cela se fasse dans le respect de la Convention relative aux droits de l'homme*.

[73] Résolution du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Echelon) - A5-0264/2001 (2001/2098 INI) 5 septembre 2001, JO C 72E 21 mars 2002, pp. 221-229. La résolution n'a pas retenu la recommandation n° 16 du rapport, qui invitait les autorités britanniques à *faire la lumière sur leur rôle dans l'alliance UKUSA étant donné que sont établies l'existence d'un système de type Échelon et son utilisation aux fins de collecte de renseignements économiques*.

Les autres points visent à encourager l'autoprotection des citoyens et des entreprises par le développement du chiffrement et le développement de logiciels "open source", afin d'éviter la présence de "backdoors". La Commission est par ailleurs invitée à renforcer son système de chiffrement.

En conclusion, une des plus importantes remarques du rapport et de la résolution a été de souligner l'absence de contrôle et de recommander la mise en place d'un organe de contrôle parlementaire sur les activités de renseignements.

3. Les déclarations du Conseil et de la Commission un an après[74]

Le 23 octobre 2002, le Conseil et la Commission font rapport au Parlement européen sur les suites données à la résolution du 5 septembre 2001. Au nom de la présidence danoise, M. Haarder souligne que le rapport Schmid a eu le grand mérite de propager la prise de conscience des questions de sécurité des télécommunications et que la présidence danoise œuvre au renforcement de la sécurité des communications des personnes physiques. En particulier, il rappelle la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.[75] Il souligne le travail encore à faire pour l'accroissement de l'utilisation du cryptage et pour l'amélioration de la sécurité informatique, considérée comme une priorité absolue dans le plan d'action européen commun intitulé *eEurope 2005*.

Le commissaire Liikanen souligne que la politique de la Commission se concentre sur la sécurité des réseaux et de l'information, comme prévu dans le plan *eEurope 2005*, qui *vise à renforcer l'échange d'informations et de bonnes pratiques, à créer une culture de la sécurité et un environnement de communication sûr*. Comme le représentant du Conseil avant lui, M. Liikanen mentionne la directive du 12 juillet 2002 : celle-ci *apportera un niveau élevé de protection au traitement des données à caractère personnel* en contenant *une disposition qui invite les États membres à garantir la confidentialité des communications et à interdire toute forme d'interception*.

Les deux déclarations ne soulèvent pas l'enthousiasme de l'Assemblée. M^me^ Flesch, faisant référence au règlement, observe qu'elles ne sont pas pertinentes par rapport à l'objet du débat. M. von Boetticher lui succède et pose au commissaire plusieurs questions sur l'avancement du projet pour la lutte contre l'interception ; il termine en soulignant que si la Commission persiste dans l'inaction, le Parlement pourra en tenir compte au moment de la décharge.

Plus modéré dans le ton mais tout aussi ferme quant au fond, M. Wiersma s'associe à l'intervention précédente et, déplorant l'absence du commissaire Patten, qui aurait pu présenter les suites données à l'affaire Echelon au niveau international.

Le président de la commission temporaire, M. Coelho, regrette pour sa part le sort réservé au rapport de sa commission, et notamment la décision du Bureau de ne pas promouvoir sa publication. Il considère que la situation n'a pas changé et déplore certaines positions qui suggèrent *que la lutte contre la criminalité internationale et le terrorisme se fait nécessairement au prix de nos libertés.*[76]

La position du groupe libéral est exprimée par M^me^ Plooij-van Gorsel. Elle considère nécessaire d'établir un cadre juridique pour en finir avec les pratiques illégales et pour

[74] Débats du Parlement européen du 23 octobre 2002.
[75] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, JO L 201 du 31 juillet 2002, p. 37.
[76] Concernant la lutte contre le terrorisme. Débats du Parlement européen du 23 octobre 2002.

définir clairement le concept d'"interceptions légales" *avec un bon contrôle au niveau européen*. La proposition de son groupe présente une double approche, avec, d'une part, la protection des droits et de la vie privée du citoyen et, d'autre part, la sauvegarde des intérêts économiques de l'Union via des mesures de lutte contre l'espionnage industriel.

Les intervenants des groupes qui n'avaient pas approuvé la résolution l'année précédente sont manifestement tout aussi critiques. En effet, M. Di Lello tient à souligner que *le véritable appel lancé par la commission Echelon concernait la protection des citoyens et de leur vie privée et que ne pas avoir pris aucune mesure concrète sur Echelon "constitue une délégitimation des institutions et du Parlement lui-même*.

M[me] McKenna exprime la position des Verts/ALE opposés *aux actions prises par le Conseil dans le but d'aligner les capacités d'interception des télécommunications aux nouvelles technologies et à l'adoption de la directive visant à permettre aux États membres d'adopter, entre autres, des mesures législatives prévoyant la conservation des données pendant un certain temps*.

Dans son intervention, M. Turco désapprouve l'inaction qui a suivi le rapport Schmid et souligne qu'on *continue à mettre en évidence le système anglo-américain* en sachant que ces systèmes sont utilisés dans des pays de l'UE.

M. Schmid est tout aussi insatisfait, mais se concentre davantage sur les questions spécifiques des logiciels "open source" et de la sécurité informatique à la Commission. Il espère notamment que soit encouragée la création d'un programme de cryptage "open source" afin que l'on maîtrise totalement ce nouveau programme.

4. La résolution du 7 novembre 2002

Le mécontentement qui est apparu lors du débat d'octobre prendra la forme d'une résolution adoptée une quinzaine de jours plus tard[77]. Dans celle-ci, le Parlement *déplore que ni le Conseil ni la Commission n'aient réagi de façon appropriée aux recommandations formulées par le Parlement* et *engage instamment le Conseil et la Commission à prendre toutes les dispositions nécessaires pour mettre pleinement en œuvre les recommandations contenues dans sa résolution précitée*, en rappelant les principaux points de la résolution du 5 septembre 2001, qui demandait des mesures spécifiques *pour protéger citoyens et entreprises contre le recours abusif et illégal à l'interception des communications, pour introduire encore et utiliser des systèmes et des techniques destinés à protéger la vie privée et la confidentialité des communications et pour mettre en place des mesures de lutte contre l'espionnage industriel et contre le recours abusif à la veille à la concurrence*.

Il reste intéressant de souligner que la résolution fait référence aux évènements du 11 septembre, qui, en 2001, avaient bloqué le débat : le Parlement européen *considérant les événements du 11 septembre 2001, d'autres attentats terroristes récents et l'effort international de lutte contre le terrorisme ont encore mis en lumière l'importance des recommandations formulées dans [la résolution du 5 septembre 2001], demande aux États membres de collaborer, coopérer et de coordonner leur action, entre eux et à un niveau multilatéral, en matière d'échange d'information, dans le but d'une plus grande efficacité dans la lutte contre le terrorisme et contre la criminalité internationale* et demande la conclusion d'accords internationaux spécifiques et le renforcement de la collaboration et de la coordination des services de renseignements des États dans le cadre de la PESD.

[77] Résolution du Parlement européen sur Echelon (B5-0528/2002), 7 novembre 2002, JO C E16 du 22 janvier 2004, pp. 88-89.

CONCLUSIONS

La commission temporaire sur l'affaire Echelon est une initiative politique du Parlement européen, qui rejoint les préoccupations de l'époque concernant la sécurité et la confidentialité des télécommunications et s'interroge quant à leur violation par le système Echelon. Cette démarche volontaire du Parlement se fonde sur les études de l'une de ses propres entités, le STOA. Celui-ci a su, d'une part, synthétiser les informations disponibles dans les médias internationaux concernant un programme d'interceptions impliquant des nations alliées et des États membres et, d'autre part, susciter les premières réactions parlementaires et lancer le débat politique.

L'affaire Echelon surgit dans les discussions du Parlement dans un contexte de relations transatlantiques fragilisées par des désaccords commerciaux et par la volonté de l'administration américaine de sanctionner les entreprises en relation avec des pays sous embargo (loi Helms-Burton). Et c'est donc tout naturellement que le système Echelon est mentionné pour la première fois dans une résolution consacrée en grande partie aux échanges économiques transatlantiques.

Ce contexte explique partiellement une certaine gêne de la part des institutions européennes et des principaux groupes parlementaires : en effet, comment enquêter sur le système Echelon sans porter préjudice aux relations déjà tendues avec l'allié américain ou sans mettre dans l'embarras le Royaume-Uni? Si la logique juridique qui soustend la création de la commission temporaire, en lieu et place d'une commission d'enquête, est fondée, elle témoigne également de la volonté de tuer dans l'œuf toute polémique éventuelle. À cet égard, l'abandon de la recommandation n° 16, qui appelle les autorités britanniques à faire la lumière sur leur rôle dans l'alliance UKUSA, est également révélateur.

En dépit de cette prudence, Gerhard Schmid produit un rapport confirmant l'existence du système Echelon et essayant d'en préciser les contours. Ce document pose également la question de la sécurité des télécommunications européennes et du cadre juridique garantissant leur protection.

Se pose la question des suites de l'affaire Echelon et de ses conséquences sur la position de l'Union européenne quant à l'interception et à la protection des données. L'affaire elle-même semble désormais bien oubliée : la presse ne s'en fait plus écho et les sites Internet qui lui sont dédiés ne sont plus mis à jour.

Cependant, l'Union européenne a lancé une réforme de grande envergure pour défendre l'accès aux données de ses citoyens, de ses institutions et de ses entreprises : il s'agit de mettre en place une approche globale de la protection des données, de renforcer les droits garantissant la protection de la vie privée en ligne, et d'en finir avec la coexistence de 28 lois nationales. Viviane Reding, commissaire européenne à la justice, n'a-t-elle pas déclaré : *Après les scandales d'espionnage de données des États-Unis, la protection des données est plus que jamais un avantage concurrentiel [...] L'Europe a besoin d'une loi forte et uniforme sur la protection des données qui donnera plus de garanties aux entreprises et une plus forte protection aux citoyens*[78].

En mars 2014, le Parlement affirme son soutien à ces déclarations et à la réforme-cadre proposée par la Commission, en adoptant les rapports des députés J.P. Albrecht et D.

[78] European Commission Memo 14/186 of 12 March 2014, Progress on EU data protection reform now irreversible following European Parliament vote.

Droutsas relatifs à la protection des données à caractère personnel et à leur libre circulation.[79]

La problématique conserve cependant toute son actualité avec les révélations de WikiLeaks et d'Edward Snowden, et les récentes écoutes dont ont été victimes la chancelière allemande, Angela Merkel, et les diplomates français en poste aux États-Unis.

[79] Rapport de la commission des libertés civiles, de la justice et des affaires intérieures sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), A7-0402/2013 - COM(2012)0011 – C7 0025/2012 – 2012/0011(COD) Rapporteur : Jan Philipp Albrecht ; Rapport de la commission des libertés civiles, de la justice et des affaires intérieures sur la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données - A7-0403/2013 - COM(2012)0010 – C7 0024/2012 – 2012/0010(COD) Rapporteur : Dimitrios Droutsas ; European Commission Memo 14/186 du 12/03/2014, Progress on EU data protection reform now irreversible following European Parliament vote.

INDEX

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Y

Z

ANNEXES

"Radômes" au Centre des opérations de cryptologie à la base aérienne de Misawa au Japon. Radôme est la contraction de "radar dôme", un boîtier étanche utilisé pour protéger les antennes. © Preston Keres - Source : www.kereskreatives.com.

17. Relations transatlantiques/Système Echelon

B4-0803, 0805, 0806 et 0809/98

Résolution sur les relations transatlantiques (système Echelon)

Le Parlement européen,

— vu sa résolution du 15 janvier 1998 sur les relations économiques et commerciales transatlantiques ([1]),

— vu la communication de la Commission au Conseil, au Parlement européen et au Comité économique et social sur un nouveau marché transatlantique,

— vu les conclusions du sommet États-Unis — Union européenne qui s'est tenu à Londres le 18 mai 1998,

A. considérant l'importance que revêtent la défense et le partage de valeurs communes à l'ère de la mondialisation,

B. considérant que les relations transatlantiques sont les plus intenses du monde, tant sur le plan politique qu'économique,

C. considérant que la progression et le renforcement des relations États-Unis — Europe auront pour effet d'accroître la stabilité politique et économique,

D. rappelant que s'agissant des effets extraterritoriaux des lois Helms-Burton et d'Amato, le Parlement a adopté une position très ferme,

E. eu égard à l'étude intitulée «évaluation des technologies de contrôle politique», rédigée par l'unité STOA (évaluation des choix scientifiques et techniques) pour la commission des libertés publiques;

1. insiste sur l'importance des relations États-Unis — Union européenne, basées sur une communauté d'intérêts dans les domaines de l'économie, de la politique et de la sécurité, ainsi que sur une perception commune des responsabilités et des besoins au niveau mondial;

2. considère que parmi ces objectifs politiques communs figure la promotion de la paix, de la stabilité, de la démocratie et du développement, ainsi que la volonté de faire face à des défis d'envergure mondiale au moyen d'une coopération renforcée;

3. rappelle que les relations économiques transatlantiques reposent sur les liens économiques et commerciaux les plus importants du monde, et que l'Union européenne et les États-Unis entretiennent les rapports économiques les plus vastes et les plus complexes du monde;

4. se félicite des résultats remarquables obtenus dans le cadre du nouvel agenda transatlantique (NAT), ce dont fait état la déclaration adoptée lors du sommet États-Unis — Union européenne susmentionnée; estime que dans ce contexte, le partenariat économique transatlantique (PET) constituera un instrument clé dans la progression des rapports bilatéraux;

5. considère que le prochain accord, qui sera négocié dans le cadre du PET et portera en particulier sur les accords de reconnaissance mutuelle (ARM) et les «normes équivalentes», sur les marchés publics et la propriété intellectuelle, devrait avoir pour effet de réduire considérablement les litiges à caractère bilatéral sur des questions de réglementation, et donner lieu à un processus de «convergence en matière de réglementation»;

6. encourage l'initiative «People-to-People links» (liens entre les peuples) qui, en promouvant les contacts dans le monde des affaires, contribue de manière appréciable à démanteler les barrières existant dans le commerce transatlantique;

7. insiste toutefois sur le fait que la législation extraterritoriale des États-Unis, et en particulier les lois Helms-Burton et d'Amato, demeurent inacceptables aux yeux de l'Union européenne; demande au Congrès des États-Unis d'intervenir rapidement en vue d'abolir de telles lois et, en tout état de cause, d'accorder les dérogations requises;

([1]) JO C 34 du 2.2.1998, p. 139.

8. demande à être tenu informé dans le détail des implications de l'accord dans la perspective de futures négociations sur l'AMI, dans la mesure où cet accord codifie certains des principes de base du projet AMI, tels que l'expropriation et la compensation;

9. accueille favorablement la déclaration commune faite par la délégation pour les relations entre le Parlement européen et le Congrès des États-Unis sur le renforcement du dialogue interparlementaire en vue de l'instauration d'un partenariat transatlantique équilibré et bénéfique pour les deux parties; considère dès lors que les échanges s'inscrivant dans le cadre interparlementaire devraient être considérablement renforcés;

10. est conscient du rôle crucial que joue la coopération internationale, grâce aux moyens de surveillance électronique, lorsqu'il s'agit de mettre un terme ou d'empêcher les activités des terroristes, des trafiquants de drogue et du crime organisé;

11. reconnaît toutefois également qu'il est essentiel que l'on puisse s'appuyer sur des systèmes de contrôle démocratique en ce qui concerne le recours à ces technologies et les informations obtenues;

12. demande que de telles technologies de surveillance fassent l'objet d'un réel débat ouvert, tant au niveau national qu'à celui de l'Union européenne, et soient soumises à des procédures garantissant une responsabilité sur le plan démocratique;

13. réclame l'adoption d'un code de conduite destiné à garantir la réparation d'erreurs ou d'abus;

14. estime que l'importance croissante du réseau Internet, et, plus généralement, des télécommunications à l'échelle mondiale et en particulier le système Echelon, ainsi que les risques de leur utilisation abusive appellent l'adoption de mesures de protection des informations économiques et d'un cryptage efficace;

15. charge son Président de transmettre la présente résolution à la Commission, au Conseil et au Congrès des États-Unis.

---

18. Gestion des déchets

A4-0235/98

Résolution concernant la communication de la Commission au Parlement européen et au Conseil concernant l'application des directives 75/439/CEE, 75/442/CEE, 78/319/CEE et 86/278/CEE sur la gestion des déchets (COM(97)0023 – C4-0368/97)

Le Parlement européen,

– vu la communication de la Commission COM(97)0023 – C4-0368/97,

– vu l'article 5 du traité CE,

– vu ses résolutions du 8 avril 1992 sur la mise en œuvre de la législation communautaire en matière d'environnement [1] et du 14 mai 1997 sur la communication de la Commission relative à la mise en œuvre du droit communautaire de l'environnement [2],

– vu le rapport de la commission de l'environnement, de la santé publique et de la protection des consommateurs (A4-0235/98),

A. considérant son engagement en faveur d'un développement durable en tant qu'objectif prioritaire de l'Union européenne,

B. considérant que l'application efficace du droit communautaire en matière d'environnement constitue une condition fondamentale pour parvenir à un développement durable,

---

(1) JO C 125 du 18.5.1992, p. 122.
(2) JO C 167 du 2.6.1997, p. 92.

EP
PE

302764 28. III. 2000

Paul Lannoye
Député au Parlement Européen
Président du Groupe des Verts/ALE

Bruxelles, le 27 mars 2000

Madame la Présidente,

J'ai l'honneur, par la présente, au nom des signataires du texte joint de vous transmettre la demande de constitution d'une commission temporaire d'enquête pour examiner les allégations d'infraction au droit communautaire (en vertu de l'article 151 du règlement) due à l'existence et aux utilisations présumées du système Echelon.

La liste des signataires est à ce jour limitée à 170 (soit plus que le quorum requis de 157) mais tous les députés n'ayant pu être contactés, il va de soi qu'elle devrait rester ouverte jusqu'à ce que la demande soit examinée par la conférence des présidents.

Vous remerciant à l'avance du suivi que vous voudrez bien réserver à cette demande je vous prie d'accepter, Mme la présidente, mes respectueuses salutations.

Paul Lannoye
Président du GVPE/ALE

PE 288.908/BUR

FR

Bureau ASP 08G 206 - Rue Wiertz
1047 BRUXELLES - Tél. 02/284.56.95
Téléfax 02/284.96.95
E-mail : PLannoye @ europarl.eu.int

Rue Basse-Marcelle, 28
5000 NAMUR
Tél. 081/23.09.69
Téléfax 081/23.18.47

FR

Demande de constitution (en vertu de l'article 151 du Règlement) d'une commission temporaire d'enquête pour examiner *les allégations d'infraction au droit communautaire* due à l'existence et aux utilisations présumées du système *Echelon*

motivation

Un rapport de STOA, (Scientific and technological Options Assessment), réalisé à la demande de la Commission des libertés publiques, publié en octobre 1999 et intitulé : « *development of surveillance technology and risk of abuse of economic information* » fait état de l'existence d'un système appelé *Echelon* qui permettrait à la NSA (*National Security Agency*) des USA, d'intercepter les télécommunications privées (téléphones fixes et portables, télécopieurs, courriers électroniques) sur l'ensemble de la planète. L'un des principaux postes de surveillance, qui concerne l'Europe, serait situé à Menwith Hill, dans le Yorkshire, au Royaume-Uni.
Ce système d'espionnage, créé à l'origine à des fins militaires se serait reconverti sur des cibles politiques et économiques au profit non seulement des Etats-Unis mais également du Canada, de la Nouvelle Zélande, de l'Australie et du Royaume-Uni.

Les informations contenues dans ce rapport ont récemment reçu confirmation, grâce à la publication de documents top secret déclassés par la NSA. Leur contenu représente pour le moins des «***allégations d'infraction au droit communautaire***», au sens de l'article 151 du Règlement, relatif à la constitution de commissions temporaires d'enquête.

En effet, l'article 286 du TCE soumet au *contrôle d'un organe indépendant*, l'application des *actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* et confirme les obligations des Etats membres en vertu du droit dérivé, en l'occurrence, les directives 95/46/CE et 97/66/CE.

Ainsi la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23/11/1995) spécifie en son article 1 paragraphe 1: «***Les Etats membres assurent, conformément à la présente directive, la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel*** ».

La directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO L 024 du 30/01/1998) est encore plus clairement concernée : « ***les prestataires de service doivent prendre les mesures appropriées pour assurer la sécurité de leurs services*** » (considérant 15) ; « ***des mesures doivent être prises pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen d'un réseau public de télécommunication ou d'un service de télécommunications accessible au public*** » (considérant 16) ; « ***lorsque les droits des usagers et des abonnés ne***

sont pas respectés, la législation nationale doit prévoir des recours juridictionnels ; (...) des sanctions doivent être infligées à toute personne, qu'elle relève du droit privé ou du droit public, qui ne respecte pas les mesures nationales prises en vertu de la présente directive » (considérant 25). Quant à l'objet de la directive, il consiste en «***l'harmonisation des dispositions des Etats membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des télécommunications***... » (article 1 paragraphe 1). En ce qui concerne la confidentialité des communications, l'article 5 paragraphe 1 de ladite directive stipule : ***« Les Etats membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunication ou de service de télécommunications accessibles au public. En particulier, ils interdisent à toute personne autre que les 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, conformément à l'art. 14 paragraphe 1».***

Or, s'il est vrai que les directives susmentionnées ne s'appliquent qu'aux politiques et activités relevant du droit communautaire, l'on peut légitimement considérer que les Institutions et organes communautaires, en tant que prestataires de services, ont manqué à leur devoir de «***prendre les mesures appropriées pour assurer la sécurité de leurs services*** » . D'autre part, on peut tout aussi légitimement considérer que l'existence d'un système d'espionnage économique au profit, notamment, d'un Etat membre aux dépens des autres Etats membres, constitue une infraction au droit communautaire, notamment à l'article 10 du TCE : « ***Les Etats membres prennent toutes les mesures générales ou particulières propres à assurer l'exécution des obligations du présent traité ou résultant des actes des institutions de la Communauté. Ils facilitent l'accomplissement de sa mission. Ils s'abstiennent de toutes mesures susceptibles de mettre en péril la réalisation des buts du présent traité. »*** De même le titre VI (ex titre V) du TCE «règles communes sur la concurrence, la fiscalité et le rapprochement des législations» prévoit à l'article l'article 81.1 (ex 85.1) que : « ***Sont incompatibles avec le marché commun et interdits tous accords entre entreprises, toutes décisions d'associations d'entreprises et toutes pratiques concertées, qui sont susceptible d'affecter le commerce entre Etats membres et qui ont pour objet ou pour effet d'empêcher, de restreindre ou de fausser le jeu de la concurrence à l'intérieur du marché commun***... ». Or, les allégations d'espionnage industriel, pratiqué via le système *Echelon* aux dépens d'entreprises du continent européen, lesquelles auraient de ce fait perdu des contrats importants au profit d'entreprises anglo-saxonnes, représentent une distortion de concurrence dans le marché intérieur et partant, une violation de la législation communautaire.

Par ailleurs, l'article 6.2 du TUE stipule que « ***l'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*** » dont l'article 8 en particulier sanctionne le respect du droit à la vie privée. A ce propos, le rapprochement des législations nationales relatives au traitement des données à caractère personnel, qui est le but de la directive 95/46/CE «***ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif***

de garantir un niveau élevé de protection dans la Communauté » (Directive 95/46/CE, considérant 10).

Toujours selon la même directive, «***les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.*** » (considérant 11). Ces principes sont également protégés par la convention 108 du Conseil de l'Europe relative à la *protection des personnes à l'égard du traitement automatisé des données à caractère personnel.*

Ensuite, les articles 11 et 12 (ex J1 et J2) du TUE peuvent également être invoqués : « ***les Etats membres œuvrent de concert au renforcement et au développement de leur solidarité politique mutuelle. Ils s'abstiennent de toute action contraire aux intérêts de l'Union ou susceptible de nuire à son efficacité en tant que force de cohésion dans les relations internationales.***
Le Conseil veille au respect de ces principes. »

Notons que l'article 151 du Règlement, relatif à la constitution de commission d'enquêtes parle d'«***allégations d'infraction au droit communautaire*** ». En d'autres termes, lesdites infractions ne doivent pas être nécessairement avérées. C'est la raison même de la constitution d'une commission d'enquête, d'établir si les allégations en question sont avérées ou non fondées. En l'occurrence, l'existence d'*Echelon* est difficilement niable puisqu'elle est désormais établie par des documents top secret de la National Security Agency (NSA) récemment déclassés.

Par ailleurs, le principe de proportionnalité - sanctionné par la jurisprudence de la Cour européenne des Droits de l'homme – nous apparaît pour le moins battu en brèche du fait du déséquilibre entre les moyens mis en œuvre par le réseau *Echelon* et les buts poursuivis.

Enfin, et en vertu du principe de précaution, il nous semble non seulement légitime mais indispensable, vu les informations dont nous disposons sur l'existence d'*Echelon* et sur les risques réels ou potentiels que ce système fait peser sur l'Union européenne, ses Institutions et organes, sur certains Etats membres et entreprises, sans oublier les personnes physiques ou morales, de mener une enquête afin de séparer le vrai du faux et, pour, le cas échéant, se doter des moyens juridiques et techniques nécessaires à une protection efficace des libertés et droits fondamentaux et au plein respect du droit communautaire. Le commissaire Bangemann, interpellé par le Parlement n'a-t-il pas déclaré, au nom de la Commission, en séance plénière du 14 septembre 1998 en réponse aux inquiétudes manifestées par de nombreux députés de tous bords quant à l'existence et aux capacités d'action d'Echelon : « *Si le système se configurait de la sorte, cela constituerait une atteinte flagrante au droit, aux droits individuels des citoyens et, bien entendu, à la sécurité des Etats membres. C'est tout à fait clair. Dès le moment où on constaterait officiellement un tel état de fait, le Conseil, la Commission et le Parlement se devraient de réagir.* »

Le Parlement européen, qui par ailleurs, a contribué de façon déterminante à la diffusion des informations relatives à *Echelon*, se doit de faire la lumière sur l'existence de ce réseau et sur l'utilisation qui en est faite afin de répondre à

l'inquiétude croissante et aux questions légitimes des citoyens européens. A cette fin, il est donc proposé de constituer une commission d'enquête qui permettrait également de de dégager les responsabilités et de mettre le doigt sur les éventuels lacunes et manquements.

Nom : Prénom : Signature :

A renvoyer à Jean-Luc Robert :
STB LOW 4048
BXL PHS 2C75

Groupe V/Ale 48/48

Ahern Nuala
Auroi Danielle
Bautista Carlos
Boumedine-Thiery Alima
Bouwman Theo
Breyer Hiltrud
Buitenweg Kathalijne
Celli Giorgio
Ceyhun Ozan
Cohn-Bendit Daniel
De Roo Alexander
Echerer Mercedes
Evans Jill
Flautre Hélène
Frassoni Monica
Gahrton Per
Graefe zu Baringdorf FW
Hautala Heidi
Hudghton Ian
Isler-Beguin Marie Anne
Jonckheer, Pierre
Knörr Gorka
Kreissl-Dörfler Wolfgang
Lagendijk Joost
Lambert Jean
Lannoye Paul
Lipietz Alain
Lucas Caroline
MacCormik Neil
Maes Nelly
McKenna Patricia
Messner Reinold
Noguira Camilo
Onesta Gérard
Ortuondo Josu
Pietrasanta Yves
Rod Didier Claude
Ruehle, Heide
Schörling Inger
Schroder Ilka
Schroedter Elisabeth
Sörensen Patsy
Staes Bart
Turmes Claude
Vander Taelen Lucas
Voggenhuber Johannes
Wyn Eurig
Wuori Matti

Groupe GUE 42/42

Ainardi Sylviane
Alavanos Alexandros
Alyssandrakis Konstantinos
Bakopoulos Emmanuouil
Bertinotti Fausto
Bordes Armonia
Boudjenah Yasmine
Brie Andreas
Cauquil Chantal
Cossutta Armando
Di Lello Giuseppe
Eriksson Marianne
Fiebiger Christel
Figueiredo Ilda
Frahm Pernille
Fraisse Geneviève
Gonzalez Laura
Hue Robert
Jove Salvador
Kaufmann Sylvia-Yvonne
Korakas Efstratios
Koulourianos Dimitrios
Krivine Alain
Laguiller Arlette
Manisco Lucio
Markov Helmut
Marset Campos Pedro
Meijer Erik
Miranda Joaquim
Modrow Hans
Morgantini Luisa
Papayannakis Michail
Puerta Alonso
Schmid Herman
Seppänen Esko
Sjöstedt Jonas
Sylla Fodé
Theonas Ioannis
Uca Feleknas
Vachetta Roseline
Vinci Luigi
Wurtz Francis

Groupe PSE 15/180

Caudron Gérard
Dehousse Jean-Maurice
Désir Harlem
Duhamel Olivier
Ferreira Anne
Garot Georges
Gui-Quint Catherine
Hazan Adeline
Iivari Ulpu
Lienemann Marie-Noelle
Myller Riitta
Nair Sami
Roure Martine
Savary Gilles
Seguro Antonio

Groupe PPE 11/232

De Mita Ciriaco
Deprez Gérard
Ebner Michl
Grosch Mathieu
Hansenne Michel
Kauppi Piia-Noora
Korhola Eija-Riitta
Matikainen Marjo
Thyssen Marianne
Vatanen Ari
Wijkman Anders

Groupe ELDR 4/51

De Clerck Willy
Di Petro
Ries Frédérique
Stercks Dirk

Groupe UEN 28/30

Abitbol
Andrews
Angelilli
Berlato
Berthu
Camre
Caullery
Collins
Coûteaux
Crowley
de La Perriere
Fini
Fitzsimon
Gallagher
Hyland
Kuntz
Marchiani
Montfort
Muscardini
Musumeci
Nobilia
Pasqua Charles
Poli Bortone
Queiro
Ribeiro e Castro
Segni
Souchet
Varaut
Thomas-Mauro
Turchi

Groupe EDD 12/16

Bernié Jean-Louis
Belder Bas
Esclopé Alain

Blokland Johannes
Bonde Jens-Peter
Farage Nigel
Holmes Michael
Krarup Ole
Mathieu Véronique
Okking Jens Dyhr
Sandbaek Ulla
Saint-Josse
Titford Jeffrey
van Dam Rijk

Groupe TDI 6/18

Bonino Emma
Cappato Marco
Dell'Alba Gianfranco
Della Vedova Benedetto
Dupuis Olivier
Turco Maurizio

****

Signatures effectives : 170
Quorum : 157

Parlement Européen
La Présidente

Monsieur Romano PRODI
Président de la Commission européenne
Rue de la Loi, 200
B-1049 BRUXELLES

302946 30.III.2000

Monsieur le Président,

Le 30 mars prochain, le Conseil et la Commission présenteront au Parlement Européen leur position quant à la question de l'interception des télécommunications évoquée lors de l'audition sur la protection des données qui s'est déroulée les 22 et 23 février dernier.

Cette question ayant déjà fait l'objet de nombreuses questions écrites et orales au cours des deux dernières années, je vous saurai gré, dans l'intérêt d'un meilleur débat, si la Commission pouvait développer essentiellement les points suivants, à savoir la nécessité :

1. d'assurer aux citoyens européens, indépendamment de leur nationalité, une protection conforme à l'art. 8 de la Convention européenne sur la protection des droits de l'homme et aux dispositions pertinentes adoptées sur la base des Traités communautaires et de l'Union ;

2. de s'assurer que toute activité d'interception des télécommunications respecte la jurisprudence de la Cour des droits de l'homme quant à la nécessité d'une proportionnalité entre l'ingérence dans la vie privée et l'intérêt public, ce qui justifierait l'interception des communications des citoyens de l'Union ;

3. d'établir sur la base des principes cités aux paragraphes précédents une norme européenne assurant que les exigences de la « sécurité européenne » soient compatibles avec celles de la « citoyenneté européenne » et prévoyant que toute forme d'interception soit notifiée aux Etats membres où se trouvent les personnes interceptées ;

4. que toute mesure adéquate soit prise par les institutions européennes pour éviter des interceptions par des pays tiers et pour établir des rapports périodiques sur les problèmes éventuellement rencontrés ; ceux-ci seraient soumis au Parlement européen conformément à l'annexe 7 de son règlement ;

5. de rendre plus simple et efficace l'action des autorités qui assurent la protection des données au niveau de l'Union par l'unification progressive des structures (Autorité prévue par l'art. 286 du TCE, Autorité Schengen, Europol, Convention douanière, ...) et le renforcement au plus haut niveau possible des standards de protection ;

6. d'adopter les mesures technologiques (câblage, cryptographie,...) pour contrecarrer les interceptions en provenance de l'extérieur de l'Union ainsi que les mesures législatives et financières nécessaires pour développer les outils et le savoir-faire informatique européens dans ce domaine ;

7. de s'assurer que chaque Etat de l'Union, conformément aux obligations de coopération loyale prévues par les articles 10 du TCE et 11, par. 2 et 29 du TUE, informe les autres Etats membres ainsi que les Institutions de l'Union de la portée de ses accords avec des pays tiers en matière d'interception des télécommunications.

Convaincue, Monsieur le Président, que vous partagez nos préoccupations quant à la nécessité que l'Union se dote dans les meilleurs délais d'un cadre législatif qui puisse, d'une part, renforcer la confiance entre ses Etats membres et, d'autre part, protéger d'avantage la vie privée de ses citoyens, je vous remercie de l'attention que vous voudrez bien accorder à cette question.

Je vous prie d'agréer, Monsieur le Président, l'expression de ma haute considération.

Nicole FONTAINE

Annexe

Le Président

Strasbourg, le 13 avril 2000

Madame Nicole FONTAINE
Présidente du Parlement européen
STRASBOURG

Madame la Présidente,

Concerne : Proposition de constitution d'une commission temporaire au vu de l'article 150, paragraphe 2, du Règlement.

Les auditions qui ont eu lieu les 22-23 février 2000 à la commission des Libertés publiques et concernant la protection des données personnelles, ont fait apparaître :

1. La confirmation de l'existence du système d'interception des communications connu sous le nom de ECHELON dont le fonctionnement est décrit dans le rapport STOA publié sous le titre "development of surveillance technology and risks of abuse of economic information" ;

2. La participation d'au moins un Etat membre au dit système ;

3. La possibilité que par ce système soient mise en oeuvre des activités d'interception et de suveillance à des fins différentes de celles autorisées par l'article 8 de la Convention européenne pour la sauvegarde des droits de l'homme et par conséquent, en violation des articles 6, parag. 2 , des articles 11 et 12 du Traité de l'UE, de l'article 286 du Traité de la CE et des principes contenus dans les directives CE/1995/46 et CE/1997/66 du PE et du Conseil sur les traitements des données personnelles et sur la protection de la vie privée dans le secteur des télécommunications ;

4. La vulnérabilité des systèmes et des moyens de communication et l'inadaptation des instruments de transmission et de cryptage des informations face à la possiblité d'abus de la part de pouvoirs publics ou privés ;

5. L'insuffisance des législations en matière de protection de données et l'absence de cohérence des dispositions concernant la coopération entre les Etats membres dans cette matière.

PARLEMENT EUROPEEN • rue Wiertz 60 • B-1047 BRUXELLES • TEL (32 2) 284 5490 • FAX (32 2) 284 9490

Compte-tenu des déclarations du Conseil et de la Commission du 30 mars dernier :

- Considérant qu'il est nécessaire de prévoir un large éventail de mesures à différents niveaux afin de faire face aux risques mis en évidence par le système ECHELON et afin de garantir les droits fondamentaux des citoyens européens ;

- Je propose que la Conférence des Présidents recommande la constitution d'une commission temporaire au vu de l'article 150 du paragraphe 2 du Règlement qui, mettant ensemble les compétences des commissions Libertés publiques, Affaires étrangères et Industrie, puisse s'attaquer à bref délai à l'ensemble des problèmes mis en exergue dans le rapport sur le système ECHELON.

La commission temporaire devrait avoir le mandat de proposer :

Des initiatives politiques pour une coopération plus loyale entre les Etats membres auxquels devra être demandé de rendre publique leurs accords avec les pays tiers sur ce sujet (cette perspective est renforcée en vue de l'élargissement aux nouveaux pays) ;

Des initiatives pour empêcher à des pays tiers toute forme d'interception sur le territoire de l'Union allant au-delà des exigences de la lutte commune au crime organisé ; des actions nécessaires afin que la protection de la vie privée soit garantie à la fois au niveau des politiques commerciales et dans le domaine de lutte contre la criminalité organisée ;

Des mesures législatives pour la mise à jour et l'harmonisation des dispositions en matière de protection de données personnelles et pour la simplification et le renforcement de l'action des autorités de contrôle, dans le cadre d'une stratégie approriée visant à garantir d'une façon plus efficace les droits fondamentaux des citoyens, même en mettant un terme au sein de l'Union au dualisme des systèmes de protection des données respectivement au niveau communautaire et au niveau de la coopération judiciaire et de la police en matière pénale (Troisième Pilier) ainsi qu'à la multiplication des autorités de contrôle (Schengen, Europol, Conventions douanières...) ;

Des initiatives appropriées pour l'adoption d'outils et de technologies (cablage, cryptage...) aptes à contrecarrer les interceptions en provenance des pays tiers ; des mesures législatives et financières aptes à développer ultérieurement les instruments et les connaissances informatiques européennes dans ce secteur.

La commission temporaire pourra être composée, au vu de l'article 152 du Règlement, de la façon suivante: 21 membres dont 12 de la commission Libertés publiques, 4 de la commission industrie, 4 de la commission Affaires Etrangers et du President. Eventuellement on pourrait y inserer de representants de la commission juridique.

La commission temporaire devra, d'ici un an, proposer les mesures nécessaires afin de contrecarrer les risques pour les droits fondamentaux des citoyens et pour les intérêts des entreprises européennes suite aux abus possibles des systèmes d'interception tous azimuts des communications non limitées aux frontières nationales.

La commission temporaire s'addressera au Parlement européen avant la fin du mois de juillet 2000 au sujet des activités qu'elle aura mis en oeuvre et elle rédigera, à la fin de son mandat, un rapport detaillé sur les thèmes sumentionnés.

Je vous prie d'agréer, Madame la Présidente, mes salutations les plus cordiales.

Enrique BARÓN CRESPO

PARLEMENT EUROPEEN

COMMISSION TEMPORAIRE SUR LE SYSTEME D'INTERCEPTION ECHELON

PROCES-VERBAL

de la réunion constitutive

6 juillet 2000

STRASBOURG

La séance est ouverte à 10:42 sous la présidence de Mme Lalumière, doyenne d'âge.

1. Election du président

La présidente informe les membres de l'objet de la réunion, à savoir l'élection du président et de trois vice-présidents, et la nomination du rapporteur. Elle constate que le quorum est atteint.

M. Schmid propose la candidature de M. Coelho. La commission approuve cette cadidature à l'unanimité moins une abstention.

La présidente félicite M. Coelho pour son élection et lui passe la présidence.

2. Election du Bureau

Le président invite les membres à proposer des candidatures pour les vice-présidences.

M. Wiersma propose la candidature de Mme Berger

M. Ceyhun propose la candidature de M. McCormick

Mme Thors propose la candidature de Mme Plooij-van Gorsel.

M. Krivine propose la candidature de M. di Lello.

Le président constate que le nombre des candidatures dépasse le nombre de postes à pourvoir.

Interviennent les membres Frahm, Krivine, Ceyhun, Dimitrakopoulos, McKenna, Wiersma, Schröder. Le président rappelle les dispositions du Règlement et invite les membres à proposer des candidatures pour la première vice-présidence.

M. Wiersma propose la candidature de Mme Berger.

Mme Thors propose la candidature de Mme Plooij-van Goorsel.

Le président annonce que l'élection devra avoir lieu à bulletins secrets et invite les membres à désigner deux scrutateurs. MM. Thielemans et Dimitrakopoulos se proposent. La commission accepte ces candidatures à l'unanimité. Le président suspend la séance à 10:58. La séance reprend à 11:07.

M. Wiersma propose d'ajourner le vote. Le président rappelle que le vote est en cours et ne peut être interrompu. Mme Banotti intervient sur un aspect technique de la procédure. Les membres effectuent leur vote à bulletin secret.

Mme Plooij-van Gorsel est élue par 24 voix contre 11 à Mme Berger.

Le président et Mme Berger félicitent Mme Plooij-van Gorsel pour son élection.

Le président invite les membres à proposer des candidatures pour la deuxième vice-présidence.

M. Ceyhun propose la candidature de M. McCormick

M. McCormick est élu par acclamation.

Le président invite les membres à proposer des candidatures pour la troisième vice-présidence.

M. Krivine propose la candidature de M. di Lello.

M. di Lello est élu par acclamation.

3. Nomination du Rapporteur

Le président propose de désigner M. Schmid comme rapporteur et invite les membres à proposer d'autres candidatures.

Mme Mckenna et M. Vattimo proposent la candidature de Mme Berger. Mme Berger refuse de se porter candidate.

M. Vattimo intervient.

M. Turco se porte candidat.

MM. Wiersma et Pirker interviennent pour soutenir la candidature de M. Schmid.

7 membres demandent que le vote pour la nomination du rapporteur ait lieu à bulletin secret. Le président suspend la séance à 11:21.La séance reprend à 11:35.

Les membres effectuent leur vote à bulletin secret.

M. Schmid est désigné par 27 voix contre 7 à M. Turco et un vote blanc.

4. Communication du président

Le président rappelle le mandat de la commission, informe les membres des dispositions pratiques pour les travaux de la commission et rappelle en particulier l'importance de respecter les règles en vigueur en matière de traitement d'informations confidentielles.

5. Déclaration du rapporteur, suivie d'un échange de vues

Le rapporteur présente ses orientations pour la préparation d'un programme de travail qui sera examiné au cours de la prochaine réunion de la commission.

Mmes McKenna et Plooij-van Gorsel interviennent.

6. Date et lieu de la prochaine réunion

La prochaine réunion aura lieu à Strasbourg le 5 septembre à 17:30.

La réunion est levée à 11:54.

DELTAGERLISTE/ANWESENHEITSLISTE/ΚΑΤΑΣΤΑΣΗ ΠΑΡΟΝΤΩΝ/LIITE RECORD OF ATTENDANCE/LISTA DE ASISTENCIA/LISTE DE PRESENCE/ELENCO DEI PRESENTI/PRESENTIELIJST/LISTA DE PRESENÇAS/LÄSNÄOLOLISTA/DELTAGARLISTA

Til stede Anwesend Παρόντες Present Presentes Présents Presenti Aanwezig Lasna Närvarande	Formandskabet/Vorstand/Προεδρείο/Bureau/Ufficio di Presidenza/Mesa/Puhemiehistφ/J.L. Presidium: (*) COELHO (P), PLOOIJ-VAN GORSEL (1st VP), MacCORMICK (2nd VP), DE LELLO FINUOLI (3rd VP) Medlemmer/Mitglieder/Μέλη/Members/Diputados/Dιputιs/Deputati/Leden/Deputados/jδsenet/ Ledamöter: BANOTI, VON BOETTICHER, CEDERSCHIÖLD, DEPREZ, DIMITRAKOPOULOS, HERNANDEZ, KLAMT, MARTIN, OOSTANDER, PIRKER, ZAPPALA, BERGER, EVANS R., KARAMANOU, LALUMIERE, LUND, MANN, PAASILINNA, SCHMID, VATTIMO, WIERSMA, CEYHUN, McKENNA, KRIVINE, TURCO, BELDER Stedfortrædere/Stellvertreter/Αναπληρωτές/Substitutes/Suplentes/Suppliants/ Membri supplenti/Plaatsvervangers/Membros suplentes/Varajäsenet/Suppleanter: CORNILLET, GAWRONSKI, GIANNAKOU-KOUTSIK, MATTIKAINEN-KALLSTRÖM, NEWTON DUNN, NIEBLER, OOMEN-RUIJTEN, ROVSING, VAN HECKE ANDERSSON, CAUDRON, GEBHARDT, MARINHO, PACIOTTI, SWIEBEL, SWOBODA, TERRON I CUSI, THIELEMANS, TITLEY ANDREASEN, THORS, BOUMEDIENE-THIERY, SCHRÖDER I., LAMBERT, FRAHM, PAPYANNAKIS,

Art. 153,2	GEBHARDT, FIORI
Art. 166,3	
Art. 162,6 Endv. Deltog/Weitere Teiln./ Συμμετείχαν επίσης/Also present Participaron igualmente/ Participaient également/ Hanno partecipato altresi´/ Andere deelnemers/ Outros participantes/ Muut osallistujat/ Dessutom deltog	

* (P) =Formand/Vorsitzender/Πρόεδρος/Chairman/Prιsident/Presidente/Voorzitter/Presidente/Puhemies/Ordfφrande
(VP) =Næstform./Stellv. Vorsitz./Αντιπρόεδρος/Vice-Chairman/Vice-Prιsident/Vicepresidente/Varapuhemies Ondervoorz./Vice-Pres./Vicepres/Vice ordförande.

Til stede den/Anwesend am/Παρών στις/Present on/Prιsent le/Presente il/Aanwezig op/Presente em/Presente el/Lδsnδ/Nδrvarande den.

Efter indbydelse fra formanden/Auf Einladung d. Vorsitzenden/Με πρόσκληση του Προέδρου/At the invitation of the Chairman/Por invitación del presidente/Sur l'invitation du président/Su invito del presidente/Op uitnodiging van de voorzitter/A convite do presidente/Puhemiehen kutsusta/
På ordförandens inbjudan:

Radet/Rat/Συμβούλιο/Council/Consejo/Conseil/Consiglio/Raad/Conselho/Neuvosto/Rådet: (*)

Kommissionen/Kommission/Επιτροπή/Commission/Comisión/Commissione/Commissie/Commissão/Komissio/
Kommissionen: (*)

Cour des comptes:

C.E.S.:

Andre deltagere/Andere Teilnehmer Επίσης Παρόντες/Also present Otros participantes/Autres participants/Altri partecipanti Andere aanwezigen/Outros participantes Muut osallistujat/Övriga deltagare		
Gruppernes sekretariat Sekretariat der Fraktionen Γραμματεία των Πολ. Ομάδων Secretariat political groups Secr. De los grupos politicos Secr. Groupes politiques Segr. Dei gruppi politici Secr. Van de fracties Secr. Dos grupos politicos Puolueryhmien sihteeristö Gruppernas sekretariat	PPE-DE PSE ELDR Verts/ALE GUE/NGL UEN TDI EDD NI	SCRIBAN, SALAFRANCA VAN DE WATER VAN DEN BROUCKE ROBERT JEAN LUC BATTISTINI
Cab. Du Président		DE VICENTE, LAGARDE
Cab. Du Secrétaire Général		
Generaldirektorat Generaldirektion Γενική Διεύθυνση Directorate-General Dirección general Direction générale Direzione generale Directoraat-generaal Direcção geral Contrôle financier Service juridique Pääosasto Generaldirektorat	I II III IV V VI VII	NICKEL, LIBERATO BARAGIOLA SILVESTRO SCHOO, KARAMARCOS
Udvalgssekretariatet Ausschubsekretariat Γραμματεία επιτροπής Committee secretariat Secretaria de la comisión Secrétariat de la commission Segretariato della commissione Commissiesecretariaat Secretaria de comissão Valiokunnan sihteeristö Utskottssekretariatet		LOWE, JACOB, HELMBERG
Assist./Βοηθός		MALOUTA

* (P) =Formand/Pres./Πρόεδρος/Chairman/Président/Voorzitter/Puhemies/Ordförande
(VP) =Næstform./Vize-Pres./Αντιπρόεδρος/Vice-Chairman/Vice-Président/Ondervoorz./Vice-pres/Varapuhemies/Vice ordförande.
(M) =Medlem./Mitglied/Μέλος/Member/Miembro/Membre/Membro/Lid/Membro/Jäsen/Ledamot
(F) =Tjenestemand/Beamter/Υπάλληλος/Official/Funcionario/Fonctionnaire/Funzionario/Ambtenaar/
Funcionário/Virkamies/Tjänsteman

27. prie instamment les États membres de ratifier la Convention de Montréal dès que possible pour améliorer la protection des passagers en cas d'accident et pour permettre la mise à jour du règlement (CE) nº 2027/97 du Conseil; souligne à cet égard l'importance d'une information claire et facilement accessible à l'intention des passagers aériens sur les limitations de responsabilité applicables y compris les délais de réclamation, informations qui devraient être automatiquement fournies par les compagnies aériennes dès la réservation;

28. considère que l'accessibilité des voyages aériens doit être améliorée pour tous les passagers, notamment les passagers handicapés, les enfants et les personnes âgées;

29. se félicite de l'intention exprimée par les compagnies aériennes de mener des actions de formation de leur personnel à l'appui aux passagers en général et aux personnes à mobilité réduite en particulier;

30. invite la Commission à présenter des propositions législatives visant à interdire à toute compagnie aérienne ou aéroport de l'Union européenne d'imposer des frais supplémentaires aux personnes à mobilité réduite nécessitant une assistance pour monter dans tout aéronef ou en descendre, partout dans l'Union européenne.

Aspects sanitaires

31. considère que la santé devrait davantage être prise en compte et que les passagers aériens et l'équipage devraient être suffisamment informés sur les aspects sanitaires du voyage aérien;

32. recommande que les compagnies aériennes donnent des informations sur la santé avant le décollage dans les vols de longue distance comparables aux informations de sécurité déjà requises et que ces informations figurent sur les billets, notamment en ce qui concerne la prévention;

33. invite la Commission, de toute urgence, à débloquer des fonds du budget de la recherche communautaire pour effectuer une évaluation indépendante sur les risques possibles de santé publique pour les passagers aériens qui voyagent sur des vols long courrier, notamment la réalisation d'une étude exhaustive sur la question de la thrombose veineuse profonde; invite la Commission à effectuer cette recherche indépendante en consultation avec les compagnies aériennes de l'UE et avec les associations de consommateurs de l'UE;

34. invite les compagnies aériennes de l'Union européenne à informer les usagers sur l'espacement longitudinal des sièges pour les passagers voyageant en classe économique;

*

* *

35. charge sa Présidente de transmettre la présente résolution au Conseil et à la Commission.

---

21. Échelon

A5-0264/2001

Résolution du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Échelon) (2001/2098(INI))

Le Parlement européen,

— vu sa décision du 5 juillet 2000, portant constitution d'une commission temporaire sur le système d'interception Échelon, ainsi que le mandat de ladite commission [1],

— vu le traité CE, qui vise la mise en place d'un marché commun présentant un degré élevé de compétitivité,

[1] JO C 121 du 24.4.2001, p. 131.

— vu les articles 11 et 12 du traité sur l'Union européenne qui lient les États membres à l'obligation de renforcer et développer leur solidarité politique mutuelle,

— vu le traité sur l'Union européenne, et notamment son article 6, paragraphe 2, qui prévoit l'obligation de respecter les droits fondamentaux, ainsi que le titre V dudit traité, qui reprend les dispositions concernant une politique étrangère et de sécurité commune,

— vu l'article 12 de la Déclaration universelle des droits de l'homme,

— vu la Charte des droits fondamentaux de l'UE, dont l'article 7 garantit le respect de la vie privée et familiale et prévoit le droit au respect des communications et l'article 8 protège les données à caractère personnel,

— vu la Convention européenne relative aux droits de l'homme (ECHR), en particulier l'article 8 de celle-ci, qui protège la vie privée et la confidentialité des correspondances, ainsi que les nombreux autres traités internationaux qui protègent la vie privée,

— vu les travaux de la commission temporaire sur le système d'interception Echelon, qui a tenu de nombreuses auditions et réunions avec les experts les plus divers, en particulier avec des responsables des secteurs public et privé dans les domaines des télécommunications et de la protection des données, avec des membres des services de renseignements, des journalistes, des avocats experts en la matière, des députés des parlements des États membres, etc.,

— vu l'article 150, paragraphe 2, de son règlement,

— vu le rapport de la commission temporaire sur le système d'interception Échelon (A5-0264/2001).

Existence d'un système d'interception mondial des communications privées et économiques (Système d'interception Échelon)

A. considérant que l'existence d'un système d'interception mondial des communications fonctionnant avec la participation, en fonction de leurs capacités, des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande, dans le cadre de l'accord UKUSA, ne fait plus de doutes; qu'il apparaît vraisemblable, eu égard aux preuves disponibles et à de nombreuses déclarations concordantes provenant d'individus et d'organisations d'horizons très divers, y compris de sources américaines, que le système porte le nom Échelon, cela étant toutefois un détail relativement mineur,

B. considérant qu'il est incontestable qu'il est utilisé au moins pour intercepter des communications privées et économiques, mais non militaires, et que l'analyse menée dans le cadre du rapport a montré que la capacité technique de ce système n'est peut être pas aussi grande, tant s'en faut, que ce que certains médias ont supposé,

C. considérant qu'il est dès lors étonnant, voire inquiétant, que de nombreux responsables communautaires auditionnés par la commission temporaire, notamment des commissaires européens, aient déclaré ne pas avoir connaissance de ce phénomène.

Limites du système d'interception

D. considérant que le système de surveillance repose notamment sur l'interception de communications par satellite, mais que, dans les régions à forte densité de communications, seule une très modeste partie des communications s'effectue par satellite; considérant que la majeure partie des communications ne peuvent être interceptées par des stations au sol mais uniquement par branchement sur câble ou par écoute radio, ce qui, comme les investigations effectuées dans le cadre du rapport l'ont montré, n'est possible que dans des limites très étroites; considérant que le personnel nécessaire pour analyser les communications interceptées détermine d'autres limites, et que les pays membres d'UKUSA n'ont, par conséquent, accès qu'à une partie très restreinte des communications par câble ou par radio et ne peuvent en évaluer qu'une partie encore plus limitée; considérant également que, aussi importants que soient les moyens et la capacité existants pour pouvoir intercepter les communications, il est impossible dans la pratique, eu égard au nombre très élevé de celles-ci, de toutes les contrôler de manière exhaustive et détaillée.

Existence possible d'autres systèmes d'interception

E. étant donné que l'interception des communications est un moyen d'espionnage traditionnel des services de renseignements et qu'un tel système pourrait être exploité par d'autres pays à condition qu'ils disposent des moyens financiers et des conditions géographiques nécessaires; que la France est le seul État membre de l'UE qui, grâce à ses territoires d'outre-mer, serait en mesure, des points de vue géographique et technique, d'exploiter de manière autonome un système d'interception mondial et qu'elle possède aussi l'infrastructure technique et organisationnelle nécessaire pour ce faire; qu'il existe de très nombreux indices prouvant que la Russie exploite vraisemblablement aussi un tel système.

Compatibilité avec le droit de l'UE

F. considérant que, s'agissant de la compatibilité d'un tel système avec le droit de l'UE, il y a lieu de distinguer deux cas: si ledit système n'est utilisé qu'à des fins de renseignements, il n'y a aucune contradiction avec le droit de l'UE, dans la mesure où les activités qui relèvent de la sécurité de l'État ne sont pas couvertes par le traité CE mais ne relèvent que des titres V du traité UE (PESC), qui ne contient encore aucune disposition en la matière, de sorte qu'une base fait défaut; en revanche, si le système est utilisé de manière abusive pour espionner la concurrence, il y a manquement à l'obligation de coopération loyale et atteinte à l'idée d'un marché commun où la concurrence est libre; si un État membre participe à une telle démarche, il viole le droit de l'Union,

G. considérant les déclarations faites par le Conseil lors de la séance plénière du 30 mars 2000, selon lesquelles: «le Conseil ne peut accepter la création ou l'existence d'un système d'interception des télécommunications qui ne respecte pas les règles de droit des États membres et qui viole les principes fondamentaux visant à préserver la dignité humaine».

Compatibilité avec le droit fondamental au respect de la vie privée (article 8 de la Convention relative aux droits de l'homme)

H. considérant que toute interception de communication constitue une atteinte grave à la vie privée, que l'article 8 de la Convention relative aux droits de l'homme, qui protège la vie privée, n'autorise que des ingérences destinées à sauvegarder la sécurité nationale, à condition que le droit national prévoie les dispositions afférentes, que celles-ci soient accessibles à tous et déterminent les circonstances et conditions d'intervention de la puissance publique, que les ingérences doivent en outre être proportionnées, ce qui suppose une mise en balance des intérêts, et que, en vertu de la jurisprudence de la Cour européenne des droits de l'homme, il ne suffit pas qu'elles soient opportunes ou souhaitables,

I. considérant qu'un système de renseignements qui intercepterait de manière aléatoire et en permanence les communications serait contraire au principe de proportionnalité et incompatible avec la Convention relative aux droits de l'homme; que, dans le même ordre d'idées, il y aurait violation de ladite Convention si les dispositions en vertu desquelles la surveillance des communications s'effectue sont dépourvues de base légale, si celle-ci n'est pas accessible à tous ou si elle est formulée de telle manière que la personne ne peut en appréhender les conséquences ou si l'atteinte n'était pas proportionnée; que les dispositions sur la base desquelles des services de renseignements américains opèrent à l'étranger sont en grande partie confidentielles, de sorte que le respect du principe de proportionnalité est à tout le moins douteux et qu'il y a manquement au principe d'accès au droit et de prévisibilité de ses effets énoncé par la Cour européenne des droits de l'homme,

J. considérant que les États membres ne peuvent se soustraire aux obligations qui leur incombent au titre de la Convention relative aux droits de l'homme en faisant intervenir sur leur territoire les services de renseignements d'autres pays soumis à des dispositions moins rigoureuses car cela reviendrait à priver de ses effets le principe de légalité et ses deux composantes — accès au droit et prévisibilité de ses effets — et viderait de sa substance la jurisprudence de la Cour européenne des droits de l'homme,

K. considérant que la conformité des activités légales de services de renseignements avec les droits fondamentaux suppose en outre que soient prévus des systèmes de contrôle suffisants parant au risque que comporte l'action secrète d'une partie de l'administration; que la Cour européenne des droits de l'homme a souligné expressément l'importance d'un système de contrôle efficace dans le domaine des activités des services de renseignements, ce qui fait qu'il apparaît préoccupant que certains États membres ne disposent pas d'organe de contrôle parlementaire de leurs services secrets.

Mercredi, 5 septembre 2001

Les citoyens de l'UE sont-ils suffisamment protégés face aux services de renseignements?

L. considérant que la protection des citoyens de l'UE dépend des situations juridiques qui existent dans les États membres, lesquelles sont très différentes et, dans certains cas, caractérisées par l'absence d'organe de contrôle parlementaire, ce qui fait que l'on ne saurait parler de protection suffisante; que les citoyens européens tiennent absolument à ce que leurs parlements nationaux disposent d'un organe de contrôle dûment et spécialement structuré pour surveiller et contrôler les activités des services de renseignements; que, même dans les pays où il existe un organe de contrôle, la tentation est grande de s'intéresser davantage aux activités intérieures des services de renseignements qu'à leurs activités extérieures, étant donné que, normalement, les citoyens du pays ne sont concernés que dans le premier cas; considérant que le fait d'obliger les services de renseignements à informer un citoyen a posteriori, par exemple cinq ans après l'interception, que ses communications ont été interceptées, encouragerait des pratiques d'interception proportionnée,

M. considérant que, compte tenu de leur dimension, des stations de réception satellitaire ne peuvent être construites sur le territoire d'un pays sans son assentiment,

N. considérant qu'en cas de coopération entre services de renseignements dans le cadre de la PESC ou de la justice et des affaires intérieures, les institutions seraient appelées à mettre en place des dispositions de protection suffisantes pour les citoyens européens.

Espionnage économique

O. considérant qu'il relève des missions des services de renseignements à l'étranger de s'intéresser aux données économiques telles que développement de branches, évolution du marché des matières premières, respect d'embargos, respect des dispositions relatives à l'approvisionnement en biens à usage mixte, etc., et que c'est la raison pour laquelle les entreprises exerçant des activités dans ces domaines sont fréquemment surveillées,

P. considérant que les services de renseignements des États-Unis s'occupent non seulement de problèmes économiques généraux mais aussi qu'ils interceptent des communications d'entreprises dans le contexte de passation de marchés, justifiant cela en invoquant la lutte contre les tentatives de corruption; considérant que cette pratique porte en elle le risque que des informations soient utilisées non pas pour lutter contre la corruption mais à des fins d'espionnage concurrentiel même si les États-Unis affirment ne pas pratiquer celui-ci; que le rôle de l'Advocacy Center du ministère américain du commerce n'est toujours pas absolument clair et qu'un entretien avec cet organisme, qui devait contribuer à la clarification, a été refusé,

Q. considérant qu'une convention en matière de lutte contre la corruption de fonctionnaire a été adoptée en 1997 dans le cadre de l'OCDE, laquelle prévoit que la corruption est passible de sanctions internationales, de sorte que dans les cas d'espèce la corruption ne saurait justifier l'interception de communications,

R. considérant qu'il est toutefois intolérable que des services de renseignements soient utilisés pour l'espionnage de concurrence, espionnant des entreprises étrangères pour procurer des avantages concurrentiels aux entreprises nationales, mais qu'il n'est pas prouvé, même si cela est souvent avancé, que le système d'interception mondial soit utilisé à cette fin,

S. considérant que, lors de la visite effectuée aux États-Unis par une délégation de la commission temporaire, des sources autorisées ont confirmé le rapport Brown, indiquant que 5 % des informations collectées grâce à des sources non publiques sont utilisées à des fins économiques; que les mêmes sources estiment que cette surveillance pourrait permettre aux entreprises des États-Unis d'emporter jusqu'à 7 milliards de dollars de marchés,

T. considérant que les données sensibles se trouvent principalement à l'intérieur des entreprises, de sorte que l'espionnage consiste notamment à tenter d'obtenir des informations par le truchement de leurs collaborateurs ou de personnes infiltrées et, de plus en plus, en pénétrant dans les réseaux informatiques, que ce n'est que lorsque les données sensibles sont acheminées vers l'extérieur par câble ou

par radio (satellite), qu'un système de surveillance des communications peut être utilisé pour espionner, trois cas pouvant se présenter:

- entreprises travaillant dans trois zones horaires, de sorte que les résultats intérimaires peuvent être envoyés d'Europe en Amérique puis en Asie,
- vidéoconférences d'entreprises multinationales se déroulant par satellite ou par câble,
- négociations de marchés importants sur place (construction d'usines, d'infrastructures de télécommunications, de systèmes de transport, etc.) lorsqu'il faut en référer à la maison mère à partir du site sur place,

U. considérant que, d'une manière générale, les petites et moyennes entreprises n'ont pas suffisamment conscience des risques et de la sécurité et ne reconnaissent pas les dangers de l'espionnage économique et de l'interception des communications,

V. considérant que le sens de la sécurité n'est pas toujours très développé dans les institutions européennes (hormis à la Banque centrale européenne, à la direction générale des relations extérieures du Conseil et à la direction générale des relations extérieures de la Commission), et qu'il y a donc lieu d'agir.

Possibilités de protection

W. considérant que la sécurité des entreprises ne peut être assurée qu'en protégeant l'ensemble de l'environnement de travail ainsi que tous les moyens de communication servant à transmettre des informations sensibles; que les systèmes de cryptage sûrs à prix abordable sont suffisamment nombreux sur le marché européen; que les particuliers doivent, eux aussi, être engagés à crypter leur courrier électronique, un courrier non crypté s'assimilant à une lettre sans enveloppe; que, sur Internet, on trouve des systèmes conviviaux qui sont mis à la disposition des particuliers, parfois même gratuitement.

Coopération entre services de renseignements de l'UE

X. considérant que l'UE est convenue de coordonner la collecte du renseignement dans le cadre du développement d'une politique de sécurité et de défense tout en poursuivant la coopération avec d'autres partenaires dans ces domaines,

Y. considérant que le Conseil européen a décidé en décembre 1999 à Helsinki de se doter d'une capacité militaire européenne plus efficace afin de pouvoir s'acquitter de l'ensemble des missions de Petersberg dans le contexte de la PESC; qu'il a en outre décidé que, pour atteindre cet objectif d'ici à 2003, l'Union devait être en mesure de déployer rapidement des troupes d'environ 50 à 60 000 hommes qui seraient autonomes, disposant des capacités de commandement, de contrôle et de renseignements nécessaires; que les premiers pas dans la voie de la mise en place d'une telle capacité autonome en matière de renseignements ont déjà été franchis dans le cadre de l'UEO et du comité politique et de sécurité,

Z. considérant qu'une coopération entre services de renseignements de l'UE apparaît souhaitable car, d'une part, une politique commune de sécurité excluant les services secrets serait absurde et, d'autre part, cela comporterait de nombreux avantages d'ordre professionnel, financier et politique; que cela serait en outre conforme à l'idée d'un partenariat à égalité de droits avec les États-Unis et pourrait regrouper l'ensemble des États membres au sein d'un système mis sur pied dans le respect de la Convention des droits de l'homme; qu'un contrôle par le Parlement européen devrait, dans ce cas, être assuré,

AA. considérant que le Parlement européen met actuellement en œuvre le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission [1], en modifiant les dispositions de son règlement relatives à l'accès aux documents sensibles.

[1] JO L 145 du 31.5.2001, p. 43.

Mercredi, 5 septembre 2001

Conclusion et modification de traités internationaux en matière de protection des citoyens et des entreprises

1. affirme, sur la base des informations recueillies par la commission temporaire que l'existence d'un système d'interception mondial des communications fonctionnant avec la participation des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande, dans le cadre de l'accord UKUSA, ne fait plus de doute;

2. invite le Secrétaire général du Conseil de l'Europe à proposer au comité des Ministres de déterminer s'il serait opportun d'adapter la protection de la vie privée garantie à l'article 8 de la Convention relative aux droits de l'homme aux méthodes de communication et aux possibilités d'interception modernes, et ce dans un protocole additionnel ou dans le contexte de la réglementation relative à la protection des données, dans le cadre d'une révision de la Convention afférente, étant entendu que cela ne saurait déboucher sur un abaissement du niveau de protection assuré par la Cour européenne des droits de l'homme ni sur une réduction de la souplesse nécessaire pour suivre l'évolution;

3. demande aux États membres dont les dispositions législatives réglementant le pouvoir d'interception des services secrets créent des discriminations en matière de protection de la vie privée de garantir à tous les citoyens européens les mêmes garanties légales en ce qui concerne la protection de la vie privée et la confidentialité de la correspondance;

4. invite les États membres de l'Union européenne à mettre en place une plate-forme européenne appelée à examiner les dispositions relatives à la garantie du secret de la correspondance et des communications, à se mettre d'accord sur un texte commun garantissant la protection de la vie privée, telle qu'elle est définie à l'article 7 de la Charte européenne des droits fondamentaux, à tous les citoyens européens sur le territoire des États membres et garantissant en outre que les activités des services de renseignements s'effectuent dans le respect des droits fondamentaux et, partant, des conditions énoncées au chapitre 8 du rapport de la commission temporaire du Parlement européen, en particulier du point 8.3.4, en vertu de l'article 8 de la Convention relative aux droits de l'homme; souligne la nécessité d'élaborer des normes communes plus adaptées aux exigences de protection des droits fondamentaux des citoyens de l'Union, qui soient plus ambitieuses que celles garanties par l'article 8 de la Convention européenne des droits de l'homme;

5. invite les États membres à adopter, lors de la prochaine conférence intergouvernementale, la Charte des droits fondamentaux en tant qu'instrument contraignant et pouvant faire l'objet de recours afin d'améliorer le niveau de protection des droits fondamentaux, notamment en ce qui concerne la vie privée;

6. invite les États membres du Conseil de l'Europe à adopter un protocole additionnel permettant à l'Union d'adhérer à la Convention relative aux droits de l'homme ou d'envisager d'autres moyens d'éviter les conflits de jurisprudence entre la Cour européenne des droits de l'homme et la Cour de justice des Communautés européennes;

7. demande, en attendant, aux institutions de l'Union européenne, dans le cadre de leur sphère de compétence et d'action respective, de mettre en application les droits fondamentaux établis par la CEDH et les protocoles y afférents, ainsi que par la Charte;

8. invite le Secrétaire général des Nations unies à charger l'organe compétent de l'Organisation de présenter des propositions visant à adapter l'article 17 de la Convention internationale relative aux droits civils et politiques, qui garantit la protection de la vie privée, aux innovations techniques;

9. estime nécessaire la négociation et la signature d'une convention entre l'Union européenne et les États-Unis établissant que chacune des deux parties respecte à l'égard de l'autre les dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises applicables à ses propres citoyens et entreprises;

10. invite les États-Unis à signer le protocole additionnel à la Convention internationale relative aux droits civils et politiques afin de rendre possibles, en cas de violation, les recours individuels devant la commission des droits de l'homme prévue par la Convention; invite les ONG américaines compétentes, notamment l'ACLU (American Civil Liberties Union) et l'EPIC (Electronic Privacy Information Center) à faire pression en ce sens sur le gouvernement américain.

Action législative nationale en matière de protection des citoyens et des entreprises

11. demande instamment aux États membres de vérifier la conformité aux droits fondamentaux, tels qu'ils sont définis dans la Convention relative aux droits de l'homme et dans la jurisprudence de la Cour européenne des droits de l'homme, de leur législation relative aux activités des services de renseignements et, au besoin, de lui apporter les adaptations nécessaires;

12. invite les États membres à se doter d'instruments contraignants garantissant une protection effective des personnes physiques et morales contre toute forme d'interception extralégale de leurs communications;

13. invite les États membres à rechercher un niveau uniforme de protection vis-à-vis des activités des services de renseignements et, à cette fin, à élaborer un code de conduite (voir paragraphe 4) en fonction du niveau de protection national le plus élevé, les citoyens concernés par les activités d'un service de renseignements étranger appartenant généralement à un autre pays, c'est-à-dire aussi à un autre État membre;

14. invite les États membres à négocier avec les États-Unis un code de conduite analogue à celui de l'UE;

15. invite les États membres qui ne l'ont pas encore fait à garantir un contrôle parlementaire et juridictionnel adéquat de leurs services secrets;

16. invite le Conseil et les États membres à mettre en place d'urgence un système de contrôle démocratique de la capacité de renseignements européenne autonome ainsi que des autres activités de renseignements communes ou coordonnées au niveau européen; suggère que le Parlement européen joue un rôle important dans ce système de contrôle;

17. invite les États membres à mettre en commun leurs moyens d'interception des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement, de la lutte contre le terrorisme, la prolifération nucléaire ou le trafic international de stupéfiants, dans le respect des dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises, sous le contrôle du Parlement européen, du Conseil et de la Commission;

18. invite les États membres à conclure avec les pays tiers une convention visant à renforcer la protection de la vie privée des citoyens de l'Union, convention dans laquelle toutes les parties s'engagent à ce que, en cas d'interception pratiquée par l'une d'entre elles dans un autre pays signataire, la première informe ce dernier des actions envisagées.

Mesures de lutte contre l'espionnage économique

19. invite les États membres à examiner si des dispositions du droit européen et international permettraient de lutter contre l'espionnage économique et la corruption visant à obtenir des marchés, notamment si une réglementation dans le cadre de l'OMC serait possible, qui tiendrait compte des distorsions de concurrence causées par de telles pratiques, par exemple en prévoyant la nullité de tels marchés; invite les États-Unis, l'Australie, la Nouvelle-Zélande et le Canada à se joindre à cette initiative;

20. invite les États membres à s'engager à inclure dans le traité CE une clause interdisant l'espionnage économique et à ne pas pratiquer l'espionnage économique entre eux, directement ou sous couvert d'une puissance étrangère qui pourrait intervenir sur leur sol, et à ne pas autoriser une puissance étrangère à mener des activités d'espionnage à partir du territoire d'un État membre de l'Union, afin de respecter l'esprit et la lettre du traité CE;

21. invite les États membres à s'engager, au moyen d'un instrument clair et contraignant, à ne pas pratiquer l'espionnage économique, proclamant ainsi le respect de l'esprit et de la lettre du traité CE; demande aux États membres de transposer ce principe contraignant dans leur législation nationale régissant les services de renseignements;

22. invite les États membres et le gouvernement des États-Unis à nouer un dialogue franc sur la collecte de renseignements économiques.

Mesures concernant l'application du droit et le contrôle de celle-ci

23. lance un appel aux parlements nationaux qui ne disposent pas d'organe de contrôle parlementaire des services de renseignements pour qu'ils se dotent d'un tel organe;

24. invite les organes de contrôle nationaux des services secrets à accorder une grande importance, dans l'exercice de leur pouvoir de contrôle, à la protection de la vie privée, que la surveillance concerne les ressortissants nationaux, les citoyens d'autres États membres de l'UE ou ceux de pays tiers;

25. invite les États membres à s'assurer que leurs dispositifs de renseignements ne sont pas utilisés abusivement pour collecter des renseignements dans le cadre de la concurrence, au mépris de l'obligation de coopération loyale des États membres ainsi que de l'idée d'un marché unique fondé sur la libre concurrence;

26. invite l'Allemagne et le Royaume-Uni à subordonner l'autorisation d'interception, sur leur territoire, de communications par les services de renseignements des États-Unis à la condition que cela se fasse dans le respect de la Convention relative aux droits de l'homme, c'est-à-dire conformément au principe de proportionnalité; que la base juridique soit accessible et que les effets soient prévisibles pour les personnes; et qu'un contrôle efficace soit prévu, étant donné qu'ils sont responsables de la conformité avec les droits de l'homme des activités de renseignements autorisées ou tolérées sur leur territoire.

Promotion de la protection des citoyens et des entreprises

27. invite la Commission et les États membres à informer les citoyens et les entreprises qu'il est possible que leurs communications internationales soient, dans certaines circonstances, interceptées; demande instamment que cette information s'assortisse d'une assistance pratique en matière de conception et de mise en œuvre de mesures de protection globales, englobant la sécurité des techniques d'information;

28. invite la Commission, le Conseil et les États membres à élaborer et à appliquer une politique efficace et active en matière de sécurité de la société de l'information; demande instamment que, dans le cadre de cette politique, une attention particulière soit accordée à la sensibilisation de tous les utilisateurs des systèmes de communication modernes en ce qui concerne la protection des informations confidentielles; demande en outre que soit mis en place un réseau européen coordonné d'organismes capables de fournir une assistance pratique en matière de conception et de mise en œuvre de stratégies de protection globale;

29. invite la Commission et les États membres à élaborer des mesures de promotion, de développement et de fabrication de matériels et de logiciels de cryptage européens et surtout à soutenir les projets visant à développer des logiciels de cryptage conviviaux dont le texte-source soit publié;

30. invite la Commission et les États membres à promouvoir des projets de logiciels dont le texte-source soit publié («open-source software»), étant donné qu'il s'agit là de la seule manière de garantir qu'ils ne comportent pas de «backdoors»;

31. invite la Commission à définir une qualification du niveau de sécurité des logiciels destinés à l'échange de correspondances électroniques en plaçant les logiciels dont le code source n'est pas publié dans la catégorie la moins fiable;

32. invite les institutions européennes et les administrations publiques des États membres à recourir systématiquement au cryptage du courrier électronique afin de faire de celui-ci la règle, à terme;

33. invite les institutions communautaires et les administrations publiques des États membres à prévoir la formation de leur personnel et la familiarisation de celui-ci avec les nouvelles technologies et les techniques de cryptage en organisant les stages et les cours de formation nécessaires;

34. demande que la situation des pays candidats fasse l'objet d'une attention particulière; demande que ceux-ci soient aidés s'ils ne sont pas en mesure de se doter des moyens de protection nécessaires faute d'indépendance technologique.

Autres mesures

35. invite les entreprises à coopérer davantage avec les services de contre-espionnage, à leur signaler les attaques extérieures relevant de l'espionnage économique, afin d'accroître leur efficacité;

36. invite la Commission à faire réaliser une analyse de sécurité destinée à préciser ce qui doit être protégé et à faire élaborer un schéma de protection;

37. invite la Commission à actualiser son système de cryptage, une modernisation s'imposant d'urgence, et demande aux autorités budgétaires (Conseil et Parlement) de prévoir les moyens financiers à cette fin;

38. propose que sa commission compétente élabore un rapport d'initiative sur la sécurité et la protection du secret dans les institutions européennes;

39. invite la Commission à assurer la protection des données dans le contexte du traitement interne de celles-ci et à renforcer la protection des documents non accessibles au public;

40. invite la Commission et les États membres à investir, dans le cadre du 6e programme-cadre de recherche, dans les nouvelles technologies de cryptage et de décryptage;

41. demande qu'en cas de distorsion de concurrence due à des aides d'État ou à un recours abusif à l'espionnage économique, les États préjudiciés informent les autorités et les organes de contrôle de l'État d'origine de ces activités pour qu'il soit mis fin à celles-ci;

42. invite la Commission à proposer la création, en coopération étroite avec les entreprises et les États membres, d'un réseau européen et coordonné de centres de conseil, notamment dans les États membres qui ne possèdent pas de tels organes, en matière de sécurité de l'information dans les entreprises qui, à côté de la sensibilisation, aurait pour mission d'apporter une aide pratique;

43. estime opportun d'organiser un colloque non limité à l'Union sur la protection de la vie privée face à la surveillance des télécommunications afin de créer une plate-forme permettant aux ONG d'Europe, des États-Unis et d'autres pays d'examiner les aspects transfrontaliers et internationaux et de coordonner les activités et démarches;

*

* *

44. charge sa Présidente de transmettre la présente résolution au Conseil et à la Commission, ainsi qu'au Secrétaire général et à l'Assemblée parlementaire du Conseil de l'Europe, aux gouvernements et aux parlements des États membres et des pays candidats, aux États-Unis d'Amérique, au Commonwealth d'Australie, à la Nouvelle-Zélande et au Canada.

"Le citoyen est relativement sans défense face aux systèmes étrangers. Le besoin de protection est donc plus grand encore dans ce domaine. Par ailleurs, il convient de ne pas perdre de vue qu'en raison du caractère particulier des services de renseignements, les citoyens de l'UE peuvent être concernés par les activités de plusieurs services de renseignements en même temps. Une protection uniforme conforme aux principes démocratiques serait souhaitable." (Rapport A5-264/2001 de Gerhard Schmid sur le système d'interception Echelon).

"[...] *techniquement c'est effectivement possible et dès lors que c'est possible peu m'importe si cela a été fait ou n'a pas été fait, ce qui m'importe c'est qu'on se protège et que ce n'est pas la France ou l'Allemagne ou les Pays-Bas qui vont se protéger isolément, c'est bien un problème de l'Union européenne"* (Déclaration d'Arthur Paecht, rapporteur de la commission de la défense nationale et des forces armées, Assemblée nationale française, devant la commission Echelon, 28 novembre 2000).

Cette étude, la première de la *Série sur l'histoire du Parlement européen,* retrace les travaux du Parlement et, plus particulièrement, de sa commission temporaire sur le système d'interception Echelon, à la suite de la révélation de l'existence d'un système d'espionnage géré par les États-Unis et conçu pour des cibles non militaires: gouvernements, organisations et entreprises de presque tous les pays.

Les études de la *Série sur l'histoire du Parlement européen* se fondent essentiellement sur les documents conservés et mis à disposition du public par les Archives historiques du Parlement européen.

Publication de
L'Unité Archives historiques
Direction générale des services de recherche parlementaire

PE 538.877
ISBN: 978-92-823-6001-9
DOI: 10.2861/69522
CAT: QA-02-14-934-FR-N