

DE LA FICTION À LA RÉALITÉ : LE PROGRAMME D'ESPIONNAGE ÉLECTRONIQUE GLOBAL « ECHELON » ET LA RESPONSABILITÉ INTERNATIONALE DES ÉTATS AU REGARD DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME (1)

PAR

Dimitri YERNAULT

ASSISTANT — CHARGÉ DE RECHERCHES
CENTRE DE DROIT PUBLIC
UNIVERSITÉ LIBRE DE BRUXELLES

« Dans un système applicable à tous les citoyens, la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée » (2).

Bruxelles, le 4 septembre 2000.

1. Aux frontières du réel, le virtuel ? — *« NetForce »*, la nouvelle série de romans de Tom Clancy, maître actuel du « technothriller », narre les exploits dans un futur proche d'un centre américain de surveillance électronique dépendant du F.B.I.. Un passage illustre fort bien les tentations auxquelles les autorités en quête de renseignements peuvent facilement succomber. Un membre de l'équipe s'est introduit dans le système informatique du méchant :

« Il y avait tout un fourbi dans le tiroir : transactions monétaires louches, lettres d'amour illicites, photos porno, les trucs habituels que les gens cherchent à plan-

(1) Le présent article repose sur une documentation à jour au 31 août 2000. Il constitue la version complète d'une étude présentée sous forme abrégée dans le numéro d'octobre 2000 du *Journal des Tribunaux* — *Droit européen* sous le titre « 'Echelon' et l'Europe ». Que les rédactions des deux revues en soit remerciées ainsi que Pierre KLEIN dont les précieuses observations n'ont peut-être pas contribué à raccourcir le texte, malgré ses souhaits, mais ont certainement mené à l'enrichissement de la présente analyse.

(2) Cour européenne des droits de l'homme, arrêt *Leander c. Suède* du 26 mars 1987, § 51. Même principe dans les arrêts *Malone c. Royaume-Uni* du 2 août 1984, § 67; *Kruslin c. France* du 24 avril 1990, § 30; *Huvig c. France* du 24 avril 1990, § 29. Lorsque, par la suite, un arrêt est indiqué sans mention de la juridiction l'ayant rendu, c'est qu'il a été prononcé par la Cour européenne des droits de l'homme.

quer. Techniquement parlant, ce qu'il faisait n'était pas à cent pour cent légal, mais il n'allait pas l'utiliser au tribunal, il était juste en quête d'indices » (3).

Cet exemple romanesque n'est pas isolé (4). Et pour qui aime se délasser les neurones au cinéma, des films d'espionnage récents (« *Mercury Rising* » avec Bruce Willis ou « *Enemy of the State* » avec Will Smith) font aussi apparaître de temps à autres un protagoniste nouveau : la toute puissante N.S.A. ou National Security Agency, service américain de renseignement électronique, à laquelle certains prêtent un budget supérieur à celui combiné de ses frère et sœur bien mieux connus, sur le plan de la renommée s'entend, que sont le F.B.I. et la C.I.A.

Mais c'est également au jour le jour qu'une nouvelle forme de renseignement commence à faire beaucoup parler d'elle en raison des risques que son existence et son utilisation font peser tant sur les intérêts économiques et stratégiques d'un grand nombre d'Etats et d'entreprises que sur le droit fondamental de toute personne humaine à l'intimité de sa vie privée : l'« intelligence électronique » (5).

2. L'Europe en émoi après les révélations de Duncan Campbell — L'Union européenne, après un premier document de travail commandité par le Parlement européen et divulgué le 6 janvier 1998 (première source officielle à mentionner *expressis verbis* l'existence d'Echelon (6), vit ainsi à l'heure du rapport « *Campbell* » (7). Ce rapport datant d'octobre 1999 est du à la plume d'un journaliste anglais, spécialiste du renseignement qui, après de longues années d'investigation, fut auditionné le 22 février 2000 par la Commission des Libertés du Parlement européen. Il fait état de l'existence

(3) T. CLANCY, *Net Force 2. Programmes fantômes*, Paris, Albin Michel, 1999, p. 165.

(4) Egalement W. DIEHL, *Régner en enfer*, Paris, J.C. Lattès, 2000, pp. 154-155 et 188-189.

(5) Voyez la contribution au titre évocateur de H. OBERDORFF, « La liberté individuelle face aux risques des technologies de sécurité », *Mélanges J. Robert*, Paris, Montchrestien, 1998, p. 177.

(6) V. WRIGHT, *An appraisal of technologies of political control*, document de travail de la Fondation Omega de Manchester pour le compte du panel Scientific and Technological Options Assessment (en abrégé le STOA qui conseille, dans le domaine scientifique, le Parlement européen auquel il est rattaché), 6 janvier 1998, PE 166 499, ci-après le rapport « *Wright* » (« <http://crypto-me.org/stoa-atcp.htm> »).

(7) Le rapport « *CAMPBELL* » fait partie d'un plus vaste ensemble de cinq documents de travail intitulé « *Development of Surveillance Technology and Risk of Abuse of Economic Information* » et édité pour le STOA par Dick HOLDSWORTH :

— Peggy BECKER, *Présentation et analyse*, Luxembourg, octobre 1999 (seule étude actuellement disponible en français), PE 168.184/vol. 1/5, ci-après le rapport « *Becker* » ;

— Duncan CAMPBELL, *The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common-carrier systems, and its applicability to COMINT targetting and selection, including speech recognition*, Luxembourg, octobre 1999, PE 168.184/vol. 2/5, ci-après le rapport « *Campbell* » ;

— Frank LEPREVOST, *Encryption and cryptosystems in electronic surveillance : a survey of the technology assessment issues*, Luxembourg, novembre 1999, PE 168.184/vol. 3/5 ;

— Chris ELLIOTT, *The legality of interception of electronic communications : A concise survey of the principal legal issues and instruments under international, european and national law*, Luxembourg, octobre 1999, PE 168.184/vol. 4/5, ci-après le rapport « *Elliot* » ;

— Nikos BOGOLIKOS, *The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception*, Luxembourg, octobre 1999, PE 168.184/vol. 5/5.

de plusieurs structures, nationales ou internationales, de surveillance des télécommunications dont la plus imposante semble donc être le programme désormais connu de par le monde sous le nom d'Echelon (8). Le rapport relate comment fonctionne l'accord UKUSA auxquels sont parties cinq pays anglo-saxons, qui forment l'ossature d'Echelon, à l'insu parfois des parlements nationaux, voire même des gouvernements (9). Le rapport « *Campbell* » décrit également l'ensemble des technologies d'interception de tous les types de communications électroniques. Il accorde surtout une attention toute particulière aux allégations selon lesquelles des firmes américaines auraient bénéficié d'informations sur la conduite de leur rivaux européennes grâce à la transmission d'interceptions effectuées dans le cadre d'Echelon.

L'émoi provoqué dans l'enceinte parlementaire européenne, lequel a trouvé écho dans les Parlements nationaux, résulte d'abord de ces révélations sur l'ampleur du renseignement économique et de l'espionnage industriel. Ce qui ne va pas sans susciter une certaine gêne puisqu'il est allégué que le Royaume Uni, membre de l'Union européenne, serait un soutien actif des Etats Unis qui apparaissent comme la pierre d'angle d'Echelon. Les Etats Unis et la Grande Bretagne nièrent au lendemain de l'audition de Duncan Campbell par le Parlement européen, tout espionnage à finalité économique (10). Mais le Directeur de la C.I.A. a reconnu devant le Congrès américain certaines « démarches défensives » pendant que la N.S.A. plaiderait la protection des conversations américaines contre les « intrus » (11). Et James Woolsey, ancien Directeur de la C.I.A., s'est largement répandu dans la presse pour expliquer que si son pays agissait de la sorte, c'était pour lutter contre les entreprises européennes qui recourent, selon ses dires, à la

(8) On ne sait s'il s'agit d'un acronyme ou non. D'après Margaret NEWSHAM, qui serait une ancienne d'Echelon, dont les propos ont été recueillis par les journalistes danois Bo ELKJAER et Kenan SEEBERG (« <http://cryptome.org/echelon-baby.htm> »), le nom aurait été trouvé par la NSA et désignerait le réseau d'ordinateurs lui-même, lequel serait notamment alimenté par des satellites Vortex. En langage militaire, le terme dont l'étymologie vient du français « échelon » (barreau d'échelle) désigne un mode d'organisation et de formation des troupes; il est également employé en ce qui concerne l'organisation des entreprises (« <http://www.qainfo.se/%7EElb/echelon.htm> »).

(9) L'ancien Premier Ministre néo-zélandais David LANGE a effectivement déclaré n'avoir jamais été mis au courant de l'existence d'une base d'écoute située dans son pays (préface au livre de Nicky HAGER, *Secret Power. New Zealand's role in the international spy network*, 1996, « <http://www.fas.org/jrp/eprint/sp/sp—fl.htm> »; cet ouvrage est également crucial dans la révélation d'Echelon). Egalement Philippe RIVIÈRE, « Petits débats sur Echelon », *Le Monde Diplomatique*, avril 2000.

(10) Suite à cette première série d'auditions, le Premier Ministre britannique s'est borné à dire que son pays n'espionne pas ceux de l'Union européenne et que ses services sont soumis à de strictes règles; le Département d'Etat américain affirme que l'espionnage économique ne fait pas partie des missions des agences américaines et se refuse toujours à reconnaître l'existence d'Echelon (« Europeans Decry U.S. Electronic Intercepts », *Washington Post* 24.02.2000 : « <http://www.washingtonpost.com/wp-srv/Wplate/2000-02/24/1581-022400-idx.html> »).

(11) J. ISNARD, « La CIA et la NSA justifient les missions du réseau d'espionnage Echelon », *Le Monde* 10.03.2000.

corruption pour conquérir des marchés extérieurs et qu'il ne saurait s'agir d'espionnage (12).

Il convient évidemment de se pencher sur l'approche économique d'Echelon. Mais se limiter à celle-ci occulterait les menaces formidables qui pèsent sur le droit à la protection de la vie privée. Encore que les deux dimensions se rejoignent lorsque l'on sait que le marché du cryptage comme moyen de préserver la confidentialité des communications devient lui-même un enjeu géostratégique majeur qui oppose les Etats Unis et le Royaume Uni à l'Union européenne qui s'y montre plus favorable (13).

3. Plan : Echelon contre la vie privée — Par-delà ses aspects économiques, les deux principaux problèmes de fond suscités par Echelon tiennent dans la violation du principe de légalité qui doit présider aux ingérences dans le droit au respect de la vie privée, d'une part, et dans le caractère supposé général et exploratoire des interceptions des messages envoyés sous telle ou telle forme électronique en contrariété avec ce même droit, d'autre part. D'après le rapport « *Wright* », Echelon procéderait en effet de la sorte :

« Within Europe, all email, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York Moors of the UK. (...) The Echelon system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex to find key-words » (14).

La participation active (en tant que pays « écouteur ») ou passive (en tant que pays d'« accueil » d'une base d'interception d'une puissance tierce) à Echelon est en contrariété avec les principes fondamentaux du droit international général (souveraineté territoriale) et les normes du droit international des droits de l'homme (droit au respect de la vie privée). Au premier rang de ces normes figure la Convention européenne des droits de l'homme qui demeure, à l'heure actuelle, le moyen juridique le plus complet tant pour analyser (1^{re} partie) que pour contrer (2^e partie) Echelon (15).

(12) Communiqué de l'agence Reuters du 23.02.2000 intitulé « Ex-CIA director says US doesn't spy for companies » (* <http://biz.yahoo.com/rf/000223/bnk.html> *).

(13) Cons. l'étude très détaillée de S. ANDREWS, « Use Who Holds the Key? — A Comparative Study of US and European Encryption Policies », *Journal of Information, Law and Technology*, n° 2000-1, * <http://elj.warwick.ac.uk/jilt/00-2/andrews.html> *.

(14) Rapport « *Wright* », pp. 18-19.

(15) Les lignes qui suivent ne traitent que des possibilités de recours contre les actes d'intelligence électronique globale et sous l'angle exclusif de leur compatibilité avec l'article 8 de la Convention européenne des droits de l'homme. Un examen approfondi des divers droits nationaux en cause réglementant l'espionnage et le contre-espionnage de même que l'analyse des textes nationaux et internationaux (CEE, OCDE, Conseil de l'Europe, ONU,...) sur le traitement des données électroniques et informatiques, leur collecte, leur protection, etc. gagneraient certainement à être effectués (même si de tels textes sont régulièrement évoqués ici à titre comparatif).

La démonstration de ce que les Etats qui participeraient à Echelon, tout en étant parties à la Convention européenne des droits de l'homme, engageraient leur responsabilité internationale au regard de celle-ci suppose d'abord que soient présentés les faits (I.A.) et que soient décrites les obligations internationales auxquelles ils manquent (articles 8 et 13 de la Convention) (I.B.). L'utilité de la Convention pour analyser ce type de système de surveillance électronique étant posée, il sera alors montré qu'elle est efficace pour le contraindre parce que le caractère multinational d'Echelon ne fait pas obstacle à l'imputabilité des manquements constatés dans le chef d'Etats parties, même s'ils agissent avec des Etats non parties comme les Etats Unis (article 1^{er} de la Convention) (II.A.), et parce que toutes les conditions de recevabilité d'éventuels recours, étatiques ou individuels, devant la Cour européenne des droits de l'homme peuvent être rencontrées en dépit de son caractère global et secret (articles 33 à 35 de la Convention) (II.B.).

1^{re} Partie. — LA CONVENTION EUROPÉENNE
DES DROITS DE L'HOMME EST UN INSTRUMENT PERTINENT
POUR ANALYSER ECHOLON

A. — *Echelon, un sujet de préoccupation planétaire
pour la vie privée ?*

4. Outre les Etats Unis et d'autres Etats de par le monde, plusieurs Etats signataires de la Convention participent de près ou de loin à Echelon, ce qu'établissent un nombre grandissant de sources et qui suscite de vives polémiques (I.A.1). Malgré les réserves exprimées sur l'efficacité de la Convention au cours de l'analyse d'Echelon par certains textes européens, cette norme recèle bien plus de ressources que ce que de telles réserves laissent présager (I.A.2.).

1. *Les réactions nationales et européennes face à Echelon*

5. Par-delà les enquêtes journalistiques qui ont déclenché la polémique, des renseignements émanant des Etats concernés officiellement disponibles et, pourtant, peu utilisés permettent de recouper les premières (I.A.1.a.). Les réactions des Parlements nationaux demeurent en demi-teinte. Le Congrès américain veut en savoir plus mais ne désire guère autre chose que la protection de ses citoyens puisqu'il renforce les moyens de la NSA à l'étranger; l'Assemblée nationale française se limite surtout à la dénonciation de l'espionnage économique; le Parlement belge s'interroge depuis de

mais le parti pris est de dégager les standards européens de protection de la vie privée en général. Des considérations d'ordre procédural exposées en fin de deuxième partie militent également en ce sens.

longs mois mais a connu un débat sur l'opportunité de la saisine par la Belgique de la Cour européenne des droits de l'homme (I.A.1.b.). Deux ans et demi de débats ont par ailleurs finalement poussé le Parlement européen à décider le 4 juillet 2000 d'une commission temporaire sur Echelon dont les résultats sont très attendus (I.A.1.c.).

a) *Echelon : fantasmes supposés et indices officielles oubliés dans les pays fondateurs*

6. Le rôle central prêté à la N.S.A. et ses relais, notamment, dans des pays européens — La F.A.S. (*Federation of American Scientists*), honorable institution fondée par des participants au projet Manhattan qui avait abouti à la mise au point de la bombe atomique américaine, regroupe 55 prix Nobel œuvrant à la paix. Son site Internet rassemble bon nombre d'informations sur Echelon.

En résumé, Echelon consisterait donc en un réseau global d'ordinateurs qui recherchent automatiquement à travers des millions de messages interceptés — certaines estimations varient de 2 millions de communications par heure à 3 milliards par jour (16) — des mots-clés préprogrammés dans des conversations téléphoniques, fixes ou mobiles, des messages envoyés par fax, télex ou courrier électronique. Le « Dictionary » (surnom du réseau d'ordinateurs et des programmes informatiques de tri des messages interceptés) des stations Echelon contiendrait non seulement les mots à rechercher indiqués par l'agence de renseignement du pays mais également ceux des pays participants.

Ce réseau aux capacités fantastiques alimenterait donc des mémoires et banques de données électroniques grâce à un réseau de satellites qui couvrent l'ensemble du globe. Les stations relais et d'écoutes seraient au moins situées, si l'on en croit la carte publiée par la F.A.S., dans 7 pays : le Royaume-Uni et l'Allemagne (Europe), le Japon (Asie), l'Australie et la Nouvelle-Zélande (Océanie), le Canada et les Etats-Unis (Amérique). La

(16) Voyez l'article de Vernon LOEB, « Critics Questioning NSA Reading Habits. Politicians Ask if Agency Sweeps In Private Data », *Washington Post* 13.11.1999. Lors de la conférence « World-Information.org » qui s'est tenue les 13 et 14 juillet 2000 à Bruxelles (sous le patronage de l'UNESCO et dans le cadre de Bruxelles 2000), Duncan CAMPBELL a rapporté qu'elles étaient selon William STUDEMAN, ancien directeur de la NSA, les statistiques d'interception par la NSA il y a quelques années. Un million de conversations par satellites seraient captées par demi-heure, 6500 seraient alors retenues par sondage, 2000 rencontreraient les critères présélectionnés, 20 seraient choisies par les analystes, seulement 2 rapports étant finalement produits pour traitement ! Un tel rendement supposé n'empêche cependant pas que cette captation systématique d'un type de communications électroniques est en soi contraire au droit à la protection de la vie privée. Or, selon D. CAMPBELL toujours, les communications radio à hautes fréquences ou par micro-ondes, par satellite, par câble sous-marin, par mobilophonie et via Internet sont sous la surveillance de divers réseaux de relais. Interviewé par *La Libre Belgique* 15-16.07.2000, il estime que mises à part les conversations par fibres terrestres (pour autant que les pays concernés disposent des technologies les plus avancées), environ 80 à 90 % des communications téléphoniques internationales sont interceptées.

N.S.A. constituerait le cœur de cette structure d'interception globale des messages qui circulent partout dans le monde. Le noyau dur d'Echelon comporterait, outre la NSA, les services de renseignement électronique de quatre autres pays : le Royaume-Uni, l'Australie, la Nouvelle-Zélande et le Canada. Ces pays composeraient le système UKUSA (17), réseau d'espionnage des pays anglo-saxons né dans la foulée de la Deuxième Guerre Mondiale. La lutte contre le bloc soviétique a progressivement laissé la place à une nouvelle conception de la sécurité nationale qui englobe désormais le renseignement commercial et économique (18).

L'existence du programme Echelon semble confirmée un peu plus chaque jour (19). Il ne faut toutefois pas se faire d'illusions : d'autres structures et agences de surveillance électronique existeraient de par le monde (notam-

(17) Seule la date approximative de passation (1947 ou 1948, selon les sources) de cet accord est connue, au contraire de son intitulé exact, les lettres UK désignant vraisemblablement le Royaume Uni et USA les Etats Unis, ses premiers signataires qui auraient déjà conclu en 1943 un accord sur le renseignement en matière de communications (en abrégé le BRUSA COMINT) : « [http://fly.hiwaay.net/\(pspoole/echelon.html](http://fly.hiwaay.net/(pspoole/echelon.html) ». Le Canada aurait passé un accord spécifique avec les Etats Unis en 1948 (« <http://www.tscm.com/cseukusa.html> »). D'autres pays seraient considérés comme « *Third Party* », à savoir l'Allemagne, l'Autriche, le Danemark, l'Italie, le Japon, la Norvège, la Corée du Sud et la Turquie (interview de D. CAMPBELL dans *La Libre Belgique* 15-16.07.2000; certaines photos sont accessibles sur « <http://www.zdnet.co.uk/news/2000/ns-16204.html> »). Espagne, Grèce, Portugal et Suède sont également cités par d'autres journalistes (C. INGRAND et J. LEGENDRE, 21.06.2000, « <http://www.zdnet.fr/actu/tech/seu/a0014771.html> »), ce qui porterait à dix le nombre de membres de l'Union européenne qui collaboreraient avec Echelon sous couvert de l'OTAN. D'après les journalistes danois déjà cités, le Danemark serait également partie prenante et accueillerait une base à Aflandshage sur l'île d'Amager, la participation à un « système de surveillance globale » sans plus de précisions ayant été reconnue par le Ministre danois de la Défense.

(18) L'adresse du site de la F.A.S. est « <http://www.fas.org/irp/program/process/echelon.htm> » (à consulter pour les nombreuses autres adresses auxquelles il renvoie, ainsi que pour la reproduction du chapitre consacré à l'accord UKUSA par le livre précité de Nicky HAGER). Les sites de l'association ZDNet France (« <http://www.zdnet.fr> ») et ZDNet UK (« <http://www.zdnet.co.uk> ») demeurent les sources les plus intéressantes d'informations les plus approfondies et les plus récentes, puisqu'ils sont entièrement actualisés à la fin juin 2000. On consultera aussi les liens nombreux du site « <http://jya.com/echelon-dc.htm> », ceux du site « <http://www.qainfo.se/%7Elb/echelon.htm> » (dont les renvois aux sites officiels des agences de renseignement) et les textes plus anciens des sites « <http://www.accessone.com/%7Erivero/POLITICS/ECHELON/echelon.html> » et « <http://www.icdc.com/paulwolf/echelon.htm> ». Le quotidien *Le Monde* tient également à jour un dossier intitulé « *Echelon : les grandes oreilles mondiales* », à l'adresse « <http://www.lemonde.fr/doss/0,2324,3156-1-MIA,00.html> » ; le *Monde Diplomatique* en fait de même (« <http://www.monde-diplomatique.fr/dossiers/echelon> »). Plusieurs ressources bibliographiques sont offertes sur « <http://www.tscm.com/cseukusa.html> ». Un bon résumé ainsi qu'une carte très parlante des implantations des stations d'écoutes, qui recoupe celle de la FAS, ont été élaborés à l'occasion d'une émission spéciale sur Radio France International du 15 février 1999 (« <http://www.transnationale.org/sources/information/RFI/Default.htm> »).

(19) Voyez les pages présentées sur le site de la George Washington University qui seraient des documents déclassifiés de l'Air Intelligence Agency américaine qui tendraient à prouver l'existence d'Echelon : « <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/12-01.htm> ». Ajoute l'interview précitée (sous le titre « Echelon was my baby ») par deux journalistes danois d'une certaine Margaret NEWSHAM qui serait une ancienne d'Echelon, employée par la firme Lockheed qui aurait participé à son développement dans les années 70. Egalement le reportage du magazine « Le Point » de Télé Canada diffusé le 25 juin 2000 sur TV5.

ment en Russie, en Chine, en Allemagne, en Israël, en France, en Inde,...) (20).

L'évolution technologique aboutirait même à ce que la N.S.A. puisse développer un projet Tempest qui permettrait de capter les signaux informatiques à travers les murs quand les ordinateurs ne sont pas relayés à un réseau (21). L'U.S. Navy reconnaît développer un nouveau système de reconnaissance vocale (22). Quant au Gouvernement anglais, c'est au grand jour qu'il construit, pour une somme estimée à 25 millions de livres, un centre de surveillance des sites Internet et d'interception des courriers électroniques, s'inspirant par là du système « *Carnivore* » dont dispose le FBI américain (23).

7. Echelon par les textes — Le double jeu du Congrès américain : protéger les citoyens américains tout en accroissant les moyens de la N.S.A. — Si les renseignements publiés par la presse et une multitude de sites Internet se démultiplient souvent les uns les autres, bien d'autres éléments tangibles, dont une décision de la Commission européenne des droits de l'homme dont il sera question par après, sont accessibles de la manière la plus officielle qui soit. Une évidence qui a peut-être joué en défaveur de leur divulgation plus tôt.

Suite au refus exprimé à plusieurs reprises par le Directeur de la N.S.A. de fournir des informations sur ses activités (24), le Congrès Américain a inséré le 9 novembre 1999, dans l'*Intelligence Authorization Act for Fiscal Year 2000*, une section 309 qui oblige la N.S.A., la C.I.A. et l'Attorney General à faire rapport dans les 60 jours sur les bases légales qu'ils estiment autoriser la communauté du renseignement à procéder à des surveillances électroniques (25). C'est dire si la situation interpelle le Congrès américain quand sont en cause les intérêts américains (26).

(20) On commence même à rencontrer des allégations sur des réseaux purement privés d'écoute : « <http://www.zdnet.co.uk/news/2000/24/ns-16210.html> » ou « <http://www.wine-storage.com/dominica.html> ».

(21) Le site de l'American Civil Liberties Union est très riche de renseignements en tous genres sur Echelon : « <http://www.aclu.org/echelonwatch/links2.htm> ».

(22) Communiqué de presse de l'Office of Naval Research Public Affairs, 01.11.1999, « <http://www.fas.org/irp/program/process/991101-voice1.htm> ».

(23) N. RUFFORD, « MI6 builds new centre to read e-mails on the net », *The Sunday Times* 30.04.2000. Un tel projet nécessite la pose de matériel chez les fournisseurs d'accès à Internet et suscite la réprobation des organisations de défense des usagers et des droits de l'homme (voyez aussi *Libération* 22-23.07.2000 et *La Libre Belgique* 24.07.2000).

(24) Le droit fédéral américain applicable au renseignement et à la défense nationale est extrêmement détaillé. Il fait l'objet du titre 50 de l'U.S. Code, disponible sur le site de la Faculté de droit de l'Université de Cornell : « <http://www4.law.cornell.edu/uscode/50/ch15.text.html> ».

(25) Encore faut-il signaler que la demande du Congrès ne concerne que les communications à destination et en provenance de « United States persons » : « <http://aclu.org/echelonwatch/hr1555c.htm> » pour le texte de la section 309 et « <http://www.house.gov/barr/> » pour le communiqué de presse du représentant BARR à l'initiative de ce texte. Les résultats de ces auditions ne sont cependant pas connus, la plupart des auditions devant les Commissions du Congrès étant classi-

La Maison Blanche a par ailleurs fait de la protection des réseaux américains contre l'espionnage économique étranger une priorité stratégique majeure (27); il en va de même du renforcement de la protection de la vie privée des citoyens américains contre les attaques d'autres États, d'entreprises étrangères ou de nature criminelle (28).

Mais les États Unis, si soucieux des droits civils de leurs ressortissants, ne s'arment pas seulement vis-à-vis de supposées attaques extérieures. Ils renforcent considérablement leurs capacités d'écoute et d'interception des télécommunications à l'étranger.

Car l'*Intelligence Authorization Act for Fiscal Year 2000* (ci-après I.A.A. 2000), trop souvent lu partiellement, ne comporte pas que cette fameuse section 309. A le consulter plus attentivement, on y découvre aussi une section 502 intitulée « *Funding for Infrastructure and Quality of Life Improvements at Menwith Hill and Bad Aibling Stations* » (29). Cette innocente disposition budgétaire est pourtant l'une des preuves tangibles tendant à accréditer l'existence d'Echelon. Située dans le titre 5 de l'I.A.A. 2000 relatif aux Agences de renseignement dépendant de l'Armée, elle proroge pour les années fiscales 2000 et 2001 l'autorisation donnée depuis 1996 au Secrétaire de l'Armée de réallouer des crédits budgétaires pour la maintenance de ces deux stations et y améliorer la qualité de vie (30).

Les stations de Menwith Hill au Royaume Uni et de Bad Aibling en Allemagne, soupçonnées d'être les principales oreilles d'Echelon en Europe (31), relèvent donc bel et bien du Ministère américain de la Défense.

Celle de Bad Aibling doit être réaménagée, ce qui justifie les dispositions budgétaires ici mentionnées (32). Les autorités américaines pourraient diffi-

fiées confidentielles en la matière (R. LEMOS, « Echelon fears could force new laws for America », 29.06.2000, « <http://www.zdnet.co.uk/news/2000/25/ns-16258.html> »).

(26) L'association américaine E.P.I.C. (Electronic Privacy Information Center), basée à Washington, a introduit le 3 décembre 1999 devant la U.S. District Court for the District of Columbia une plainte pour enjoindre à la N.S.A. de fournir des renseignements sur les écoutes qu'elle aurait menées à son encontre (communiqué de presse et texte de la plainte sur « <http://www.epi-c.org/open-gov/foia/nsa-suit-12-99.html> »).

(27) *A National Security Strategy for a New Century*, Washington, Services de la Maison Blanche, décembre 1999, p. 17.

(28) *Defending America's Cyberspace — National Plan for Information Systems protection*, Washington, Services de la Maison Blanche, 2000, pp. 6-7 et 11-15.

(29) Cette disposition est très officiellement publiée dans *Public Law 106-120* du 3 décembre 1999, 113 stat. 1619.

(30) C'est la section 506 de l'I.A.A. 1996 qui a permis de telles réaffectations pour la première fois au cours des exercices 1996 et 1997 (*Public Law 104-93* du 6 janvier 1996, 109 stat. 974), la prorogation pour les exercices 1998 et 1999 ayant été effectuée par la section 502 de l'I.A.A. 1998 (*Public Law 105-107* du 20 novembre 1997, 111 stat. 2262).

(31) Voyez notamment les cartes déjà mentionnées publiées par la F.A.S., *Le Monde et Radio France International* ou encore le rapport « *Campbell* ».

(32) C'est ce qu'indique le rapport du Select Committee on Intelligence du Sénat américain du 11 mai 1999 sur l'I.A.A. 2000 alors en projet, doc. n° 106-48. Cet amendement (projet de section 306 du Sénat) a été fait sien par la Chambre des représentants dans son rapport du 5 novembre 1999, doc. n° 106-457. Les travaux préparatoires de la section 502 et de l'I.A.A. 2000

cilement nier que cette base recèle des équipements de télécommunications performants, pour ne pas dire plus, puisqu'elle fut durant le conflit entre l'OTAN et la Serbie au Kosovo le centre de toutes les transmissions des forces de l'OTAN, le rôle de la NSA ayant été déterminant. C'est du moins ce que déclarait un certain Général Wesley K. Clark devant la Commission des armées de la Chambre des Représentants le 17 février 2000 (33).

Quant à la base de Menwith Hill, il faut croire qu'elle revêt quelque importance puisque les travaux de la Chambre portant sur le budget des installations militaires de l'armée pour l'année 1998 prévoyaient d'en renforcer les clôtures de protection (sans doute pour éviter les intrusions d'activistes) mais également un crédit de 818.000 \$ pour y construire une High School (ce qui suppose un personnel et des familles d'une certaine ampleur) (34). La proposition du représentant Spence « *To authorize appropriations for fiscal years 2000 and 2001 for military activities of the Department of Defense, to prescribe military personnel strenghts for fiscal years 2000 and 2001 and for other purposes* » comportait pour sa part une section 2401 autorisant en particulier des constructions et acquisitions de terrains par les agences dépendant du Ministère de la Défense. L'on y apprend à la lecture des tableaux de bases situées hors des Etats Unis que la NSA en gère une sur le site de la Royal Air Force britannique à Menwith Hill (35).

Voici donc des éléments troublants qui confirment le plus officiellement du monde que la NSA possède bien des stations d'interception électronique à l'étranger (36), en particulier sur le continent européen, et ce en dépit des

dans son ensemble sont disponibles sur le très précieux site de l'Université de Loyola « <http://www.loyola.edu/dept/politics/intel> ».

(33) Cette audition du commandant suprême des forces de l'OTAN dans le conflit est officiellement disponible sur le site du House Armed Services Committee : « <http://www.house.gov/hasc/testimony/106thcongress/00-02-17clark.htm> ». Les écoutes à Bad Aibling seraient actuellement dirigées contre le Liechtenstein et la Suisse en vue de remonter les filières du blanchiment d'argent (information publiée le 30.06.2000 sur « <http://www.zdnet.co.uk/news/2000/25/ns-16341.html> »).

(34) Amendement n° 7 au projet intitulé « *Making appropriations for military construction, famill housing, and base realignment and closure for the Department of Defense for the fiscal year ending september 1998, and for other purposes* », doc. n° HR 105-247.

(35) Ce document (106th Congress, 1st session, 14 avril 1999, n° HR 1401) se trouve sur « <http://www.house.gov/hasc/billsandreports/106thcongress/hr1401h.htm> ». Cette proposition a débouché sur le *National Defense Authorization Act for fiscal year 2000* (Public Law 106-65 du 5 octobre 1999, 113 stat. 837) qui reprend dans sa section 2401 la liste des bases des agences dépendant du Département de la Défense nécessitant de nouvelles opérations immobilières ; seule celle de la NSA à Menwith Hill n'est plus mentionnée dans le texte adopté. En indiquant qu'il s'agit d'une base de la NSA, les travaux préparatoires du NDAA 2000 confirment ainsi explicitement le texte de l'IAA 2000 qui se rapporte aux agences de renseignement dépendant du Département de la Défense américain sans plus de précisions.

(36) La loi organique de la NSA (*National Security Agency Act of 1959*) règle d'ailleurs en détails les primes, conditions d'hébergement,... des employés civils et militaires ainsi que de leurs familles travaillant pour elle à l'étranger (« <http://www.fas.org/irp/offdocs/laws/pl086036.htm> »).

dénégations des autorités américaines (37), lesquelles ont cependant contestées par après par la chaîne de télévision NBC News (38).

Si l'on ajoute que la NSA a officiellement soutenu le dépôt par trois de ses agents d'un brevet auprès du US Patent and Trademark Office, le faisceau d'indices commence à ressembler à une forêt (39). Le brevet, enregistré le 10 août 1999 sous le n° 5,937,422, est très explicitement intitulé « *Automatically generating a topic description for text and searching and sorting text by topic using the same* » (40). Voilà qui ressemble furieusement à un logiciel de tri des messages interceptés du type « Dictionary ».

Le Congrès américain vient de faire du renforcement de la NSA une priorité stratégique majeure (41).

8. Echelon par les textes (suite) — Le Royaume Uni entre loyautés européenne et transatlantique : la cogestion anglo-américaine de la base de Menwith Hill — La collaboration la plus étroite entre Etats Unis et Royaume Uni en matière de renseignement électronique est attestée par les sources officielles britanniques. Les réponses ministérielles à un nombre important de questions écrites de membres du Parlement tant sous l'administration Thatcher que sous le gouvernement Blair confirment, voire même précisent, la place cardinale qu'occupe la base de

(37) Les dénégations américaines portent en particulier sur l'espionnage économique. Il faut pourtant bien constater qu'une directive du Président REAGAN du 4 décembre 1981, toujours d'application, prescrit notamment aux Agences qui composent « *the Intelligence Community* » de collecter, conserver et disséminer toute « *information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations* » (section 2.3.b. de l'*Executive Order 12333 — United States intelligence activities* : « <http://www.nara.gov/fedreg/eos/e12333.html> »). Sauf délégation spécifique du Secrétaire de la Défense, c'est bien la NSA qui possède le monopole du renseignement électronique sous toutes ses formes (section 1.12.b.1), ce dont elle ne se vante guère sur son site Internet où elle ne reproduit qu'un résumé de cette directive présidentielle (« <http://www.nsa.gov/about—nsa/mission.html> »).

(38) R. WINDREM, « U.S. spying pays off for business », 14.04.2000, « <http://www.msnbc.com/news/394993.asp?cpl=1> ». La rédaction de NBC rapporte que le Directeur de la NSA affirme qu'elle ne livre pas de renseignements économiques aux firmes américaines mais reconnaît ne pas savoir ce que les services des pays qui collaborent avec elles peuvent en faire. Outre les témoignages d'anciens officiels ou d'officiels en service sous couvert d'anonymat, NBC se base encore sur des documents relatifs à la transition entre les administrations BUSH et CLINTON qui ont trait à la réorientation globale de la politique du renseignement en direction de l'espionnage économique.

(39) D. CAMPBELL et R. BARRY offrent un résumé des diverses preuves connues au 30 juin 2000 sur « <http://www.zdnet.co.uk/news/2000/25/ns-16261.html> ».

(40) Le site de l'Office américain des brevets sur lequel l'enregistrement de la demande peut être trouvé est le « <http://164.195.100.11/> ».

(41) Voyez le très explicite communiqué de presse du *Senate Select Committee on Intelligence* publié le 4 mai 2000 à l'occasion de l'adoption du rapport sur l'*Intelligence Authorization Act for Fiscal Year 2001*, « <http://intelligence.senate.gov/000504.htm> ». Sans compter les systèmes embarqués sur navire ou avion, ni ceux situés dans les représentations américaines à l'étranger, certains estiment que la NSA possède des relais propres ou partagés avec d'autres services dans plus d'une quarantaine de pays dont la liste est recensée par J. WEST et W. MADSEN, « The Radome Archipelago — A Most Unusual Collection Agency », *The Village Voice* 24.02.02. 03.1999, « <http://www.fas.org/jirp/news/1999/02/radome.htm> ».

Menwith Hill pour la collecte, le traitement et la répartition de l'intelligence électronique des deux pays.

Si la pratique gouvernementale établie de longue date est de ne pas répondre aux « spéculations » relatives aux opérations de renseignement, réponse fréquente dès qu'il s'agit d'Echelon (42), le Gouvernement refuse tout autant de communiquer aux Parlement les accords régissant les relations anglo-américaines en matière de défense (43). En juin 2000, seul l'accord de 1951 sur le statut des forces de l'OTAN était disponible à la Bibliothèque du Parlement, les autres textes étant toujours considérés comme confidentiels par le Gouvernement britannique (44) qui, pour le reste, se limite à affirmer la soumission au droit anglais régissant les interceptions des services anglais et américains présents sur le territoire (45).

La justification selon laquelle la présence de la NSA se déroule dans le cadre de l'OTAN et profite à la politique de défense des membres de l'Union européenne a été récemment (cyniquement ?) avancée à la Chambre des Lords (46).

Des informations sur le personnel déployé à Menwith Hill ont été épisodiquement données (47), avant qu'il ne soit officiellement reconnu le 12 mai

(42) Notamment la réponse du Secrétaire HAZ à la question écrite de Mr BAKER (House of Commons, bulletin du 4 mai 2000, col. 200) qui invoque, comme la plupart du temps, les dispositions de l'exemption n° 1 du *Code of Practice on Access to Government Information*. Les réponses ministérielles aux questions écrites (ci-après WA) de membres des Communes (ci-après HC) ou de la House of Lords (ci-après HL), sont toutes accessibles via le moteur de recherche du Parlement (« <http://www.parliament.the-stationery-office.co.uk/> ») qui en affiche les listes (tapez « Menwith » comme objet de recherche). Elles sont citées ci-après sous forme abrégée.

(43) WA de Mr CRYER, HC 16.06.1992, col. 501; WA de Mr MADDEN, HC 14.06.1994, col. 533-534; WA de Lord KENNET, HL 20.03.1997, col. 92; WA de Mr BLUNT, HC 26.07.1999, col. 56. Une réponse du Secretary of State for Defence HAMILTON donnée en 1992 s'est cependant montrée relativement explicite : « *The United States communications facility at Menwith Hill is located on a Ministry of Defence site made available to the United States department of defence. It is an integral part of the world wide department of defence communications network but I am not prepared to comment further on its operational role. It operates with the full knowledge and consent of Her Majesty's Government* » (WA de Mr MAHON, HC 09.06.1992, col. 97).

(44) WA de Lord MARSH, HL 05.06.2000, col. 128-129.

(45) WA de Mr GOODLAD, HC 20.03.1995, col. 48; WA de Lord KENNET, HL 18.03.1999, col. 114; WA de Mr BAKER, HC 14.07.1997, col. 59.

(46) Réponse de la Baronne SYMONS OF VERNHAMDEAN à la WA de Lord KENNET, HL 11.11.1999, col. 189-190 : « *US operations on UK soil are performed with the full knowledge and consent of the UK Government and conducted with full respect for the law. Bilateral and, if necessary, confidential agreements between individual nations and third countries that allow the use of their sovereign territory are consistent with the development of the European Union's common foreign and security policy and the Declaration on European Defence agreed by the Prime Minister at St Malo. Indeed, these arrangements provide a valuable contribution to the collective security of all NATO countries and are entirely consistent with our policy of improving European defence capabilities. Whether other European countries are aware of the activities of the United States National Security Agency is a matter for them* ».

(47) WA de Mr MADDEN, HC 21.03.1996, col. 285. 1200 américains et 600 britanniques sont alors recensés, le nombre d'agents du GCHQ étant inclus mais non précisé. Les salaires des britanniques étaient remboursés par le Département US de la Défense à hauteur de 5.4 millions £ (WA de Mr MAHON, HC 18.03.1996, col. 64). Des membres de l'US Navy, de l'US Army, de l'US

2000 que le site occupait 415 militaires et 989 civils américains, ainsi que 392 civils britanniques, le nombre de membres du GCHQ (Gouvernement Communications Headquarter) n'ayant pas été communiqué pour raisons de sécurité nationale (48). Ceci n'en prouve pas moins que Menwith Hill est cogérée par les services de renseignement des deux États (49).

Le Gouvernement a aussi plusieurs fois précisé que les dépenses d'infrastructure sont à charge exclusive des autorités américaines (50). Les 23 radomes en activité (dômes de protection des antennes dont 2 supplémentaires sont en cours d'installation) sont également la propriété de celles-ci (51).

Menwith Hill n'est de surcroît pas la seule base britannique sur laquelle l'armée américaine entretient des systèmes de communications (52). Si son rôle en matière d'interception de communications n'a jamais été officiellement éclairci, cette base sert de toute façon à la collecte d'informations sur le lancement de missiles (53).

On achèvera de se convaincre de l'implication du Royaume Uni dans un réseau international de surveillance électronique en consultant le tout aussi officiel site Internet du GCHQ, destiné à promouvoir le recrutement d'analystes, de mathématiciens et autres spécialistes du cryptage. On y lit toujours que

« All GCHQ systems are linked together on the largest local area network in Europe — which is connected to other sites around the world via one of the largest wide area networks on earth » (54).

Air Force et des US Marines ainsi que du personnel civil sont présents sur le site (WA de Mr MAHON, HC 09.06.1992, col. 97 : en 1992, il n'y avait que 560 anglais).

(48) WA de Mr BAKER, HC 12.05.2000, col. 513. Comparés aux chiffres précités de 1996, ceux-ci démontrent un accroissement des américains à hauteur de 200 unités, ce qui doit sans doute dénoter un regain d'activités de la NSA à Menwith Hill.

(49) Il a été en outre précisé qu'aucune activité pouvant être considérée comme hostile aux intérêts britanniques n'était ou ne serait permise sur le site (WA de Lord JENKINS OF PUTNEY, HL 03.07.1996, col. 107), cela étant empêché par la présence de personnel anglais à tous les stades de la hiérarchie (question orale de Mr CRYER, HC séance du 25.03.1994, col. 609 et suiv; et de Mr BAKER, HC séance du 06.04.1998, col. 9).

(50) WA de Mr MADDEN, HC 24.02.1997, col. 119.

(51) WA de Mr MAHON, HC 18.03.1996, col. 63. Les 2 radomes supplémentaires sont destinés à un système de détection de missiles : WA de Mr BAKER, HC 09.11.1998, col. 74 (*infra*).

(52) La réponse aux WA de Mr SOAMES et de Mr MADDEN, HC 12.07.1995, col. 679 et 680 en cite pas moins de 18, Menwith Hill y incluse. Le Gouvernement a toutefois alors refusé de confirmer ou infirmer si les bases de la RAF de Croughton et de Chicksands étaient utilisées ou non par la NSA.

(53) Dans le cadre du programme américain *Space Based Infra Red System* : WA de Mr BAKER, HC 08.02.2000, col. 111. Le Gouvernement américain n'aurait cependant pas demandé à pouvoir y implanter d'autres systèmes de guidage et de détection de missiles en rapport avec son projet actuel de « parapluie nucléaire » : WA de la Baronne WILLIAMS OF CROSBY, HL 29.03.2000, col. 76. L'existence de ce programme n'est pas considérée comme contraire aux intérêts économiques de l'Union européenne et de ses membres (WA de Lord KENNET, HL 25.10.1999, col. 5-6). Les 2 radomes en cours de construction sont affectés à ce programme; on se demande à quoi peuvent bien servir les 23 déjà existants.

(54) « <http://www.gchq.gov.uk/textonly/about/technology.html> ».

Le Gouvernement britannique persistait, en juillet 2000, à toujours refuser de répondre aux interrogations parlementaires sur Echelon (55).

9. Echelon par les textes (suite et fin provisoire) — L'implication des autres pays anglo-saxons — Le très officiel rapport pour 1996 du Vérificateur général du Canada comportait un très long chapitre 27 intitulé « *The Canadian Intelligence Community. Control and Accountability* ». La lecture de son point 27.21 se passe de commentaires :

« The Communications Security Establishment (CSE), an agency of the Department of National Defence, is one of the main organizations devoted to providing the government with foreign intelligence. CSE analyses and reports on intercepted foreign radio, radar and other electronic emissions, referred to as signals intelligence (SIGINT), and provides this foreign intelligence to Canadian government clients. The Canadian Forces Supplementary Radio System (CFSRS) supports CSE primarily in its signals intelligence collection and analysis roles. In addition, CSE has access to allied SIGINT through reciprocal sharing agreements ».

Et le point 27.28 du même rapport lève, s'il en reste, toute ambiguïté :

« Canada has close formal intelligence relationships with a number of countries. The closest of these were forged during World War II and solidified during the Cold War. Links remain particularly strong with the United States, the United Kingdom, Australia and New Zealand. Intelligence products, including analyses and assessments, are exchanged, and technical assistance is provided by each to the others. These, and other relationships, provide Canada with information and technological resources that would otherwise be unobtainable with current resources » (56).

Voilà pour qui douterait encore de l'existence même de l'accord UKUSA et du cadre qu'il offre à la collaboration « électronique » internationale des pays anglo-saxons. S'il est vrai que l'on se perd en conjectures sur la portée réelle des capacités d'interception et de traitement d'Echelon (tel est bien le problème), son existence, ignorée d'un ancien Premier Ministre néo-zélandais (57), ne fait donc plus guère de doutes. Celle-ci a d'ailleurs été reconnue par l'Inspecteur général du renseignement et de la sécurité d'Australie qui

(55) La question avait été pourtant explicitement soulevée par Lord BACH en séance plénière, HL 19.07.2000, col. 1031-1032, à l'occasion des débats sur la compatibilité avec le droit européen du *Regulation of Investigatory Powers Bill 2000*. Appelé à se prononcer sur le rapport « Wright », le Ministre de la Défense REID a répondu très énervé à une question orale de Mr BAKER, HC séance du 06.04.2000, col. 9-10, que « *The Honourable Gentlemen would not expect me to comment on a report that I have never seen or, indeed, heard of — far less vouch for its veracity. RAF Menwith Hill is a communications facility, and there is a total integration of United States and United Kingdom staff there. There is not only parliamentary accountability but accountability through the Intelligence and Security Committee, and not least from the hon. Gentleman. Of the thousands questions he has tabled since entering Parliament — at up to £ 600 a time — more than 20 on this matter have had my personal attention* ».

(56) Les passages non en italiques sont soulignés par nous. Le rapport 1996 de l'auditeur général du Canada est accessible via « <http://www.oag-bvg.ca/> ».

(57) *Supra* dans la préface au livre de N. HAGER.

a confirmé la participation à Echelon du Defense Signals Directorate (DSD) (58).

b) *L'ambiguïté des réactions nationales face à Echelon : les cas belge et français*

10. La France, espionne et espionnée — La principale préoccupation française est l'espionnage économique. Devant l'Assemblée nationale, la Ministre de la Justice a clairement répondu le 23 février 2000 à une question du député G. Sarre sur Echelon que la collaboration des cinq pays anglo-saxons remontait à 1948 et que

« il semble, en effet, que ce réseau soit détourné à des fins d'espionnage économique et de veille concurrentielle, ce qui appelle de notre part une particulière vigilance » (59).

Cette réponse ne comportait aucune autre information sur Echelon et se bornait à recommander le cryptage des transmissions de données ainsi qu'à indiquer les divers groupes de travail œuvrant à la lutte contre la criminalité informatique.

Le député Y. Nicolin déposa début mars une proposition de création d'une commission d'enquête parlementaire en n'ayant égard qu'au problème de l'espionnage économique (60). Sur rapport de la Commission de la Défense nationale de l'Assemblée Nationale, il a été décidé de ne maintenir que la mission d'information parlementaire sur « Les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale » instaurée par la même Commission le 29 février 2000 (61). Le rapport stipule toutefois que

« les dénégations récentes des responsables politiques américains et britanniques manquent par trop de crédibilité pour qu'une analyse n'ait pas lieu sur la réalité du phénomène et les moyens de pallier ses inconvénients ».

Le choix du maintien de la mission d'information est justifié par la capacité des industriels français à faire face à l'espionnage industriel et par le caractère secret des programmes développés avec le Gouvernement. Mr. Quilès, Président de la Commission de la Défense nationale affirma à cette occasion que

(58) Rapport « Campbell », p. 7.

(59) Le compte rendu de la 1^{ère} séance de l'Assemblée du 23.02.2000 est disponible sur « <http://www.assemblee-nationale.fr/2/cr/20000132.htm> ». Voyez aussi les extraits de réponses ministérielles reproduits sur le site du groupe des Verts au Parlement européen dans le journal en ligne *Lambda*, n° 6.01 (« <http://lambda.eu.org/6xx/601.html> »).

(60) Doc. A.N., 11^e législature, 6 mars 2000, n° 2233 : « <http://www.assemblee-nationale.fr/2/propositions/pion2233.htm> ».

(61) Doc. A.N., Commission de la Défense nationale, 29 février 2000, compte-rendu n° 27 : « <http://www.assemblee-nationale.fr/2/cdef/c-rendus/c9900027.htm> ».

« selon des informations récemment publiées, la France et les Etats-Unis collaboraient depuis longtemps dans le domaine de l'écoute électronique (...) (et) qu'il importait de ne pas confondre ce qui relève de la coopération normale avec des pays alliés et l'utilisation abusive que ces pays pouvaient faire de leur propre réseau de surveillance » (62).

La mission d'information, confiée à Mr. Paecht, est actuellement à l'ouvrage. Mais les informations les plus récentes relatent que la France possède également son propre réseau d'interception électronique que la Direction Générale de la Sécurité Extérieure (DGSE) entretient à Domme en Dordogne et possède des relais dans les Emirats Arabes Unis et en Nouvelle Calédonie notamment (63). La base de lancement de l'Agence spatiale européenne à Kourou en Guyane constituerait également une station d'interception utilisée également, moyennant rétribution, avec le Bundesnachrichtendienst allemand (BND) (64).

On lit d'ailleurs dans l'avis de la Commission de la Défense nationale sur le projet de loi de finances pour 1999 qui se penchait sur le renouvellement du parc spatial militaire français que

« (le satellite Hélios 1) comprend aussi un système d'écoute électronique Euracom, réalisé uniquement dans le cadre national français » (65).

Ceci n'empêche pas que le parquet de Paris a confié à la Direction de la Surveillance du Territoire (service intérieur de contre-espionnage) une enquête préliminaire sur les éventuelles retombées d'Echelon, principalement en matière économique et, plus accessoirement, quant à la protection de la vie privée (66). Comme le souligne ironiquement un quotidien français, la DST aura fort à faire sachant que la DGSE a donc son réseau (67) et qu'elle collaborerait par ailleurs avec... la NSA (68).

11. La Belgique entre déclarations musclées et extrême retenue — Le Comité « R », organe auxiliaire du Parlement belge, qui a pour mission le contrôle des services de renseignement, n'a pu, sur foi des déclara-

(62) Rapport de M. MICHEL sur la proposition de résolution n° 2233, Doc. A.N., Commission de la Défense nationale, 6 avril 2000, n° 2270 : « <http://www.assemblee-nationale.fr/2/rap-res/r2270.htm> ».

(63) D. KAMINSKY et J. THOREL, « Frenchelon, les grandes oreilles made in France », 21.06.2000, « <http://www.zdnet.fr/actu/tech/secu/a0014768.html> » ; D. CAMPBELL et R. BARRY, « Frenchelon : First pictures of French listening post », 30.06.2000, « <http://www.zdnet.co.uk/news/2000/25/ns-16207.html> » ; J. THOREL, « Frenchelon — France has nothing to envy to Echelon », 30.06.2000, « <http://www.zdnet.co.uk/news/2000/25/ns-16281.html> ».

(64) J. GUISEL, « L'espionnage n'est plus un secret », *Le Point* 10.07.1998, reproduit sur « <http://www.adetocqueville.com/cgi-bin/loc/getzip.cgi?0+782> ».

(65) Avis du 8 octobre 1998 de la Commission de la Défense nationale sur le projet de loi de finances pour 1999, doc. A.N., n° 1114, p. 53, « <http://www.assemblee-nat.fr/2/dossiers/plf99/a1114-08.htm> ».

(66) Egalement *La Libre Belgique* 05.07.2000. Des avocats français envisagent aussi un recours devant la Cour de justice des Communautés afin de forcer les institutions communautaires à agir contre la NSA (« <http://www.zdnet.co.uk/news/2000/25/ns-16174.html> »).

(67) *Libération* 05.07.2000.

(68) *Libération* 03.04.2000.

rations de ceux-ci, que constater qu'il leur était impossible, faute de moyens, d'en savoir plus que ce que les sources ouvertes permettaient de connaître (69). Le Gouvernement belge a toutefois estimé par la bouche du Ministre de la Justice « *inacceptable* » l'existence d'Echelon dans lequel il voit une atteinte à la souveraineté nationale et une violation de la vie privée, ce qui justifie le soutien aux travaux du Parlement européen (70).

Le Ministre des Affaires étrangères a quant à lui déclaré que

« l'existence éventuelle d'un réseau d'écoute électronique mondial nommé 'Echelon' est dramatiquement problématique et mérite évidemment notre attention. Cette information provient d'une étude du Parlement européen et semble renforcer des soupçons antérieurs. Bien que les affirmations contenues dans ce nouveau rapport soient essentiellement le fait de déductions et d'interprétations déjà problématiques en soi, les Etats Unis paraissent aller dans le sens d'une confirmation de ces éléments ».

Le Ministre poursuit :

« (...) si l'existence du réseau est confirmée, j'en tirerai, après consultations gouvernementales, les conclusions nécessaires en matière de politique étrangère » (71).

Répondant le 22 février 2000 à plusieurs interpellations et questions orales devant la Commission des Affaires étrangères de la Chambre, le Ministre des Affaires étrangères a par ailleurs affirmé que

« à ma connaissance, la Belgique n'abrite pas d'installations d'écoute américaines ou britanniques, contrairement à l'Allemagne. Mais la question n'est pas encore close et je ne manquerai pas de vous informer, dès que je disposerai des éléments nécessaires à l'éclaircissement de la situation. Il importe, en effet, d'assurer l'intégrité de la Belgique » (72).

Le Comité R poursuit actuellement ses investigations. Les auditions se déroulent à huis-clos mais la presse relate cependant l'existence d'un rapport encore classifié de deux chercheurs des Facultés Notre Dame de la

(69) Rapport d'activités 1999 du Comité permanent de contrôle des services de renseignements et de sécurité, fait par MM. HORDIES et DE DONNEA, 14 février 2000, *Doc. parl.*, Chambre 50 430/001 et Sénat 2-332/1, pp. 46 à 69. Dans la presse : *Le Matin* 16.02.2000; *De Morgen* 18.02.2000; *La Lanterne* 28.02.2000. Voyez également l'interpellation de M. DELEUZE au Ministre de la Justice sur le système « Echelon » (n° 2067), Annales de la Commission de la Justice, Chambre, 26 octobre 1998; question orale de M. DELEUZE au Ministre de la Justice (n° 1745), Annales de la Commission de la Justice, Chambre, 11 janvier 1999, et la réponse du Ministre selon laquelle, à l'époque, l'enquête de la Sûreté de l'Etat n'a pas pu confirmer l'existence du programme.

(70) *De Morgen* 17.02.2000. Le Ministre répondait à une question orale du député VAN HOOBEKE posée le 13 février 2000 en Commission de la Justice de la Chambre.

(71) Annales des séances plénières, Sénat, jeudi 17 février 2000, séance de l'après-midi. Egalement *La Libre Belgique* 24.02.2000.

(72) Le compte-rendu analytique de la réunion de la Commission des Affaires étrangères de la Chambre en date du 22 février 2000 est disponible sur le site « <http://www.lachambre.be/commissions/acts/bel30f01.htm> ». Le Ministre ajoute plus loin dans le débat que « *les démarches déjà menées sur le plan diplomatique se sont révélées extrêmement délicates. On me demande de quoi je parle et je ne peux prendre le risque de lancer, sans dossier bien étayé, des démarches qui ne sont pas pertinentes* ».

Paix de Namur qui estiment que la presse a grossi l'importance d'Echelon qui ne capterait que les messages transitant par les satellites Intelsat et Eutelsat (73) (74).

12. La proposition de saisine par la Belgique de la Cour européenne des droits de l'homme contre l'Allemagne et le Royaume Uni, un débat en suspens — C'est dans ce contexte que le sénateur socialiste Philippe Moureaux a adressé au Vice-premier Ministre et Ministre des Affaires étrangères une demande d'explication débattue au Sénat lors de la séance plénière du 6 juillet 2000 (75). La demande (dont l'argumentation est semblable à celle exposée dans le présent article) repose sur la considération politique que la Belgique étant un pays plus modeste que ceux participant à Echelon et dont le Ministre avait affirmé auparavant qu'elle n'en faisait pas partie se trouverait mieux placée pour intenter une action devant des instances internationales. Une politique étrangère nettement réorientée par un changement de coalition gouvernementale milite également en ce sens selon le sénateur, les affaires Pinochet et autrichienne en attestant.

Vu le nombre de sources journalistiques et officielles convergentes sur Echelon, il fut donc proposé par Mr Moureaux que la Belgique saisisse, sur base de l'article 33 de la Convention, la Cour européenne des droits de l'homme d'une requête étatique qui serait dirigée contre l'Allemagne (parce

(73) Voyez *De Morgen* 15.05.2000 et *La Libre Belgique* 19.05.2000.

(74) L'auteur a pu consulter le Rapport d'activité complémentaire pour 1999 du Comité R, remis le 8 mai 2000, mais toujours classé confidentiel à l'heure de la rédaction de ces lignes. On remarque d'abord le nombre peu important de sources officielles ouvertes étrangères à avoir été consultées (ainsi seule la section 309 de l'IAA 2000 du Congrès américain est mentionnée; seules quelques questions parlementaires britanniques sont recensées;...). Deux seules véritables informations nouvelles figurent dans le rapport. D'une part, dans son audition du 2 mars 2000, l'administratrice-générale de la Sûreté de l'Etat confirmait la participation de fonctionnaires belges aux séminaires « ILETS » (International Law Enforcement Telecommunications Seminar) menés par le FBI américain et, notamment, les services des quinze membres de l'Union, en vue d'harmoniser les techniques d'interceptions téléphoniques; la Belgique serait ainsi le premier pays à en reconnaître l'existence. D'autre part, l'audition du 3 mars au cours de laquelle l'officier général du SGR a affirmé que « suivre » Echelon serait illégal en Belgique faute de législation sur les interceptions de sécurité (ce qui est parfaitement exact et analysé plus loin). Il s'est surtout avéré que les deux services belges ne s'échangeaient pas d'informations, que la Sûreté n'était pas équipée pour lutter contre l'espionnage économique et que le comité ministériel du renseignement ne s'est jamais saisi du dossier Echelon. Quant au rapport de MM. POULLET et DINANT (Centre de recherche Informatique et Droit de l'Université de Namur), il conclut bien à l'existence d'un réseau international de surveillance électronique dont Menwith Hill est la plaque tournante mais serait limité aux communications par satellite (1 % des communications internationales selon eux). Ils doutent également de l'existence d'une technologie de reconnaissance vocale déclenchant l'écoute et prônent le recours au cryptage. Les deux chercheurs concluent cependant à la contrariété d'Echelon, notamment, avec l'article 8 de la Convention européenne des droits de l'homme (défaut de légalité et d'accessibilité des textes le régissant, défaut de proportionnalité de la collecte de données,...) et que le droit applicable à la NSA ne protège que les citoyens américains. Ils en terminent en appelant à la mise en place d'un organisme de sécurisation des interceptions en Belgique. Ces éléments, en possession des plus hautes instances parlementaires depuis le 8 mai 2000, n'ont pas été divulgués lors de la séance plénière du Sénat du 6 juillet.

(75) Voyez *La Libre Belgique* 06.07.2000 et *De Morgen* 13.07.2000.

qu'elle ne peut plus ignorer qu'elle son territoire à disposition de la NSA qui procède à des écoutes contraires à la Convention) et le Royaume Uni (pour le même motif et en tant que partenaire actif de l'accord UKUSA). Les avantages en seraient certains : conditions de recevabilité allégées, soutien à d'éventuelles requêtes individuelles, contribution au renforcement de l'ordre public européen,...

Le débat se déroula dans une ambiance lourde. Le Président du Sénat, qui préside également la commission parlementaire de suivi du Comité R, argua de ce que celle-ci travaillait sur le cas Echelon pour affirmer qu'il ne fallait pas préjuger de ses conclusions et pour que le débat soit relancé à la rentrée parlementaire en octobre 2000.

Un parlementaire écologiste de la majorité, membre de ladite commission, estima cependant que la proposition devrait être suivie si se confirmait une atteinte aveugle et sans base légale aux droits fondamentaux et aux intérêts des entreprises.

Un sénateur de l'opposition sociale-chrétienne flamande a exprimé au contraire des doutes quant à la faisabilité d'une saisine étatique de la Cour européenne en se référant au très faible nombre de cas précédents et à la gravité des atteintes aux droits en cause, principalement ceux protégeant l'intégrité physique, qui les justifiaient. Le fait que, par exemple, la France possédant un réseau de surveillance propre devrait aussi être attaquée, ainsi que la circonstance que les Etats Unis, n'étant pas parties à la Convention, ne peuvent être attirés devant la Cour furent également soulevés par le même parlementaire pour marquer ses réserves à l'égard de la requête interétatique, celle-ci pouvant en entraîner d'autres en retour de la part des Etats visés. La Convention ne protégerait pas non plus les activités économiques, selon lui (76).

Un membre de l'opposition sociale-chrétienne francophone soutint pour sa part directement l'idée et suggéra en outre d'étudier l'opportunité de la saisine de la Cour de Justice des Communautés européennes.

Une sénatrice de la majorité demanda au Gouvernement d'apporter son soutien à la Commission de suivi du Comité R à propos de la qualification des faits et des auteurs tout en s'interrogeant sur les visites aux bases visées qu'auraient pu éventuellement rendre des militaires belges. Doutant de la volonté de la France d'investiguer au-delà de la mise en cause de ses intérêts économiques et voyant dans l'affaire Echelon un véritable test pour la politique européenne de sécurité, la parlementaire se demanda enfin si l'afflux soudain de révélations sur Echelon ne visait pas à relancer le marché du cryptage.

(76) On peut déjà objecter à ce stade vis-à-vis de ces deux dernières remarques que la Convention ne soumet à aucune réciprocité les requêtes étatiques et que la protection des activités économiques est bien assurée par son article 8. Ces points sont tous deux analysés plus bas.

Ce fut le Ministre des Télécommunications qui répondit à la place du Ministre des Affaires étrangères. Sous réserve d'éléments ultérieurs et des auditions programmées quelques jours après devant le Comité R, il rappela la condamnation de principe par le Président de l'Union européenne intervenue le 30 mars 2000, lequel aurait déclaré cependant ne pas avoir d'informations claires sur l'existence d'interceptions (77), et les courriers des gouvernements anglais et américain adressés à la Commission européenne niant tout espionnage industriel. Le Ministre attacha une importance particulière à la déclaration britannique selon laquelle le Gouvernement de Sa Majesté procédait bien à des interceptions mais en respectant le droit anglais, ce qu'il interpréta comme une reconnaissance.

Sur le plan juridique, le Ministre des Affaires étrangères belge répondit par l'entremise du Ministre des Télécommunications que le manque d'informations sur les bases légales et politiques d'Echelon rendaient « *aléatoire* » l'identification des responsabilités et le fondement d'une éventuelle plainte. Après avoir relu en substance l'article 8 de la Convention européenne des droits de l'homme (78), le Ministre résuma de façon très lacunaire la jurisprudence de la Cour sur les écoutes téléphoniques et indiqua que le droit anglais serait en conformité avec elle (79). L'argument central de la réponse ministérielle demeure cependant la présence d'Etats non européens :

« Le mécanisme de la protection européenne des droits de l'homme est peu outillé pour faire face à des systèmes transnationaux mis en œuvre par une pluralité d'Etats non européens. Il n'a pas été conçu pour poursuivre les Etats dont la responsabilité internationale simple ou pénale serait à établir » (80).

Et de conclure :

« Le Vice-premier Ministre estime que, pour la Belgique, les inconvénients d'une telle démarche l'emportent sur les avantages symboliques qui en découleraient ».

Le seul intérêt réel de la réponse du Ministre des Télécommunications tient dans les considérations qu'il a émises à titre personnel lorsqu'il a

(77) Comme cela sera vu au point e) suivant, le Président de l'Union a été bien plus précis que cela.

(78) Le Ministre des Télécommunications devait avoir un discours partiel sous les yeux puisqu'il constata que l'article 8 de la Convention ne prévoyait la préservation du bien-être économique du pays comme motif de limitation du droit à la vie privée, alors que cette disposition compte au contraire explicitement ce motif!

(79) Quand bien même le droit anglais serait-il respecté et conforme à la Convention, on voit assez mal sur base de quel principe juridique il s'imposerait aux personnes résidant sur le territoire belge!

(80) Il n'est guère aisé de démêler ce qui relèverait de la responsabilité internationale simple ou pénale, concepts inconnus. La réponse comporte également une distinction entre requête étatique individuelle et requête interétatique qui n'existe nullement dans la Convention. Il doit s'agir là d'une distinction purement politique entre une action que la Belgique mènerait seule, laquelle n'a manifestement pas les faveurs ministérielles, ou en collaboration avec d'autres Etats dont il est allégué qu'elle suppose un degré de cohésion des Etats membres de l'Union européenne, ce qui n'était absolument pas l'objet de la demande d'explications du sénateur Moureaux.

affirmé sans ambages qu'un système comme Echelon était techniquement parfaitement concevable, se cantonnant pour le reste à la plus grande prudence dans une enceinte parlementaire car « *chaque mot prononcé peut avoir des conséquences* ».

13. Le positionnement de la Belgique à l'égard d'Echelon, un débat reporté à la fin 2000? — Le sénateur qui avait introduit cette demande de saisine de la Cour de Strasbourg n'a pu que marquer sa déception et constater la faiblesse de l'analyse juridique du département des Affaires étrangères (81). Il est effectivement établi, comme le présent article le démontre dans la deuxième partie, que la Convention européenne prise dans son ensemble permet la contestation d'Echelon. La circonstance que des pays qui l'ont signée agissent de concert avec des pays qui n'y sont pas parties ne saurait en rien relever les premiers de leurs responsabilités.

Qui plus est, si cela constituait toujours aux yeux du Gouvernement belge un obstacle irrémédiable, la demande d'explications du sénateur évoquait une autre voie qui, elle, permet d'attirer tous les Etats, en ce compris les Etats Unis : la communication étatique devant le Comité des droits de l'homme de l'ONU selon la procédure prévue par l'article 41 du Pacte international relatif aux droits civils et politiques pour contrariété d'Echelon avec l'article 17 du Pacte qui protège, comme l'article 8 de la Convention européenne des droits de l'homme, le droit au respect de la vie privée (82).

Toujours est-il que la réaction britannique n'a pas tardé. L'ambassadeur du Royaume Uni a qualifié d'« *irresponsable* » la suggestion de saisine de la Cour de Strasbourg en estimant normal que son pays confie le contrôle d'Echelon à ses propres autorités car

« *Nous considérons que le Royaume Uni le fait mieux que quiconque* » (83).

Si ce n'est que ce qui est demandé aux Etats membres d'Echelon est, outre le respect des droits fondamentaux de leurs ressortissants et des personnes résidant sur leur territoire (84), de ne pas violer la souveraineté

(81) Les débats consécutifs à la demande d'explications de Mr Moureaux au Vice-Premier Ministre et Ministre des Affaires étrangères sur « la possibilité de saisine de la Cour européenne des droits de l'homme par la Belgique en raison de la contrariété du programme Echelon avec les principes de la Convention européenne des droits de l'homme » ont été fort longs. C'est pourquoi leur compte-rendu analytique (séances plénières du Sénat, session ordinaire 1999-2000, jeudi 6 juillet 2000, séance de l'après-midi, n° 2-61) a été ici résumé (voyez « <http://www.senate.be> »).

(82) Voyez *infra*, deuxième partie *in fine*, point II.B.3.

(83) *La Libre Belgique* 08.07.2000.

(84) La construction du nouveau centre de contrôle d'Internet du MI5 déjà mentionnée correspond avec l'adoption par le Parlement anglais du tout aussi contesté *Regulation of Investigatory Powers Act* ce 28 juillet 2000 (texte sur « <http://www.uk-legislation.hmso.gov.uk/acts/acts2000/00023-a.htm> »). Les critiques ont été nombreuses tout au cours de son élaboration notamment quant à certaines obligations de livrer des clés de cryptage, quant aux cas où un mandat du Secretary of State n'est pas requis, quant aux surcoûts générés pour l'industrie,... (« <http://www.olswang.com/telecoms/talking-telecoms/reg-powers-bill.html> »). La conformité

d'Etats qui n'ont pas consenti sur leur territoire à ce que les premiers procèdent à des interceptions électroniques. Qui plus est, le droit belge prohibe encore toutes les écoutes administratives sur le territoire belge (85). Si ce n'est que ce qui est demandé aussi est de ne plus soumettre les individus à des écoutes n'obéissant qu'à des règles, en admettant qu'elles existent, insuffisamment accessibles et prévisibles et que ses individus n'ont de toute façon pas à connaître quand ils ne relèvent pas de la juridiction américaine ou britannique. Si ce n'est qu'il est surtout demandé, dans tous les cas, qu'il soit mis fin aux écoutes aveugles à l'aide de systèmes d'interception globaux (86).

Le Premier Ministre belge s'est engagé le 19 juillet 2000 devant la commission parlementaire de suivi du Comité R à revenir devant elle fort des conclusions d'un groupe de travail interministériel destiné à étudier comment protéger les télécommunications belges. La commission entendra pour sa part Mr Solana, représentant européen de la politique extérieure et de sécurité commune et des spécialistes du cryptage (87). Le Premier Ministre a encore indiqué qu'il était trop tôt pour prendre des initiatives comme la saisine de la Cour européenne des droits de l'homme, préférant attendre les conclusions de la commission de suivi ainsi que celles de la commission temporaire instituée le 5 juillet par le Parlement européen (88). Ce qui n'empêche pas non plus la Belgique de se doter d'une loi sur la criminalité informatique, en cours de discussion au Parlement, extrêmement critiquable à plus d'un égard (89).

c) *La Commission temporaire du Parlement européen sur Echelon : quête de vérité ou report des funérailles ?*

14. Les valseuses hésitations des autorités communautaires depuis déjà deux ans et demi — Cela fait quelques années que le Parlement

avec la Convention européenne des droits de l'homme a été au cœur des débats parlementaires en raison de la condamnation prononcée dans l'arrêt *Halford contre Royaume Uni* rendu par la Cour européenne des droits de l'homme en 1997 (C. BARCLAY et G. G. GRIMWOOD, *The Regulation of Investigatory Powers Bill. Bill 64 of 1999-2000*, Research Paper 00/25, Library of the House of Commons, 3 mars 2000). L'affirmation de la conformité du droit britannique avec la Convention ne doit pas faire oublier non plus la condamnation intervenue dans l'arrêt *Khan contre Royaume Uni* rendu le 12 mai 2000, analysé par la suite.

(85) *Infra* I.B.1.a.2°.

(86) Un des problèmes les plus prégnants posés par Echelon est la capacité que cette structure offre aux pays participants de contourner leurs propres lois sur la protection de la vie privée en ayant recours aux interceptions opérées par les services d'autres pays. L'exemple de deux Ministres du gouvernement THATCHER mis sur écoutes par les services canadiens au profit du Premier Ministre est souvent cité, notamment sur « <http://www.zdnet.co.uk/news/2000/25/ns-16176.html> ».

(87) *Le Soir* 20.07.2000.

(88) *De Morgen* 31.07.2000.

(89) B. GILSON, « La Belgique bientôt à l'heure du téléficage », *Le Matin* 03.08.2000. Un des ses aspects, critiqué plus loin, a trait à la possibilité de procéder à des saisies informatiques extraterritoriales.

européen essaye d'en savoir plus sur Echelon (90). Sa tâche ne doit pas être facilitée par le fait que le Royaume-Uni est un membre actif des accords UKUSA (91), que l'Allemagne accueille une station Echelon et que la France possède de son côté des services visiblement fort actifs aussi (92). Qui plus est, les 15 pays de l'Union Européenne seraient eux-mêmes engagés dans la confection d'un système de surveillance globale de lutte contre la criminalité; ils collaboreraient avec le F.B.I. dans le cadre de séminaires juridiques sur le droit des télécommunications (93).

Le débat sur Echelon devant les instances communautaires remonte pourtant au 6 janvier 1998 lorsque fut déposé un document de travail, déjà évoqué, commandité par le Parlement à Monsieur Wright de la Fondation Omega basée à Manchester. Ce document passait en revue un éventail de nouvelles technologies de surveillance en vue du contrôle politique de groupements supposés factieux ou terroristes mais parfois aussi de tout un chacun (armes non léthales, militarisation de l'équipement de la police, privatisation des prisons, techniques d'interrogatoire poussées, contrôle visuel du trafic routier...). Echelon apparaît au détour du chapitre consacré aux développements récents des technologies de surveillance.

Le Parlement européen s'est d'abord inquiété de l'espionnage électronique et de ses retombées économiques dans le cadre des relations transatlantiques à la rentrée 1998 (94).

Saisi des cinq nouveaux rapports rédigés pour le STOA à la fin 1999, la Commission juridique et du marché intérieur et la Commission des Libertés et des droits des citoyens Parlement ont procédé, les mardi 22 et mercredi 23 février 2000, à des auditions sur le thème de « L'Union européenne et la

(90) Voyez l'interview du député européen travailliste Glynn FORD publié dans *Libération* du 21.04.1998, le journal relatant également l'historique de la découverte d'Echelon.

(91) Un article du journaliste milanais Claudio GATTI (paru dans *Il Mondo* et traduit dans *Le Courrier International* du 2 avril 1998) relate qu'en 1998 le Gouvernement THATCHER, estimant trop élevé le coût de la mise en place d'un réseau de surveillance purement britannique, se serait engagé dans un protocole ultra-secret à verser aux Etats Unis une contribution de 500 millions de livres en échange de la réorientation de trois satellites-espions de la N.S.A. sur des cibles concernant ses intérêts, pour 4 mois par an maximum, la N.S.A. conservant la priorité en cas de crise (« <http://dept-info.labri.u-bordeaux.fr/álvarado/papers/echelon.html> »).

(92) Sur tous ces points, voyez le dossier très complet publié par *Le Monde* du 23 février 2000 et en particulier la carte figurant à la page 3 qui corrobore la présence de relais Echelon au Japon et en Allemagne, pays « amis » des 5 parties à l'accord UKUSA (voyez *supra*, le site Internet de la F.A.S.).

(93) Voyez les premières pages du rapport « Campbell » ainsi que l'audition, citée plus haut, de l'administratrice-générale de la Sécurité belge.

(94) La résolution du Parlement européen du 16 septembre 1998 sur les relations transatlantiques (point 14) estime que les risques d'abus découlant en particulier d'Echelon appellent l'adoption de mesures de protection des informations économiques et d'un cryptage efficace (*J.O.C.E.* 12.10.1998 C 313, p. 98). Les pays européens et les instances communautaires hésitent, faute de preuves définitives de l'espionnage économique et industriel américain, à compromettre leurs relations avec les U.S.A. (P. RIVIÈRE, « Tentations policières dans le cyberspace. 'Grandes oreilles' américaines », *Le Monde Diplomatique*, mars 1999, p. 21).

protection des données » (95). Le Parlement européen s'est penché à cette occasion sur le désormais fameux rapport « *Campbell* ».

Au cours de la séance plénière du 30 mars 2000 consacrée à Echelon, nombreuses furent les interventions des partisans, des opposants ou des mitigés. Deux discours sortent cependant du lot en ce qu'ils étaient centrés sur le respect de la Convention européenne des droits de l'homme : la déclaration de Mr Liikanen pour la Commission et l'intervention du député PSE britannique, Mr Evans.

Fidèle aux positions pour le moins attentistes que la Commission a toujours eues à l'égard d'Echelon (96), le Commissaire Liikanen rappela que les Directives sur la protection de la vie privée laissaient aux Etats le soin de traiter des questions de sécurité nationale, les affaires intérieures et de justice faisant partie du « troisième pilier » qui ne ressort pas aux compétences de l'Union en tant que telle. La politique du renseignement demeurant une compétence nationale, la Commission avait toutefois adressé un courrier au gouvernement britannique qui répondit en substance que les services anglais respectaient le droit anglais qui prévoit avec précision les cas dans lesquels il peut être recouru aux écoutes téléphoniques. Le droit anglais, qui ménage un contrôle parlementaire, aurait reçu l'aval de la Commission européenne des droits de l'homme. Mr Liikanen dit également avoir reçu des clarifications du Gouvernement américain déniaient tout espionnage industriel et la transmission à des firmes privées du bénéfice d'interceptions électroniques (97). Les démentis américain et britannique ne surprennent guère quelques semaines après qu'ils aient déjà été formulés. Encore qu'ils ne portent pas (ou plus ?) sur l'existence d'Echelon en soi. Quant à l'allégation britannique selon laquelle le droit anglais est conforme à la Convention, elle est pour le moins tempérée par la troisième condamnation du Royaume Uni, le 12 mai 2000, par la Cour européenne des droits de l'homme en raison des défaillances du droit applicable aux écoutes (98).

L'intervention du député Evans dans la foulée de cette déclaration préalable s'achève de façon étonnante :

(95) Voyez l'ordre du jour des auditions sur « L'Union européenne et la protection des données » des 22 et 23 février 2000 et le procès-verbal de la Commission des Libertés, PE 285.915.

(96) L'ancien Commissaire européen M. BANGEMAN déclarait encore en février 1998 devant le Parlement européen ne pas vouloir réagir sur base de simples soupçons mais que « *si ce système existait jamais, ce serait une attaque intolérable contre les libertés individuelles, la concurrence et la sécurité des Etats* » (propos rappelés dans *Le Soir* 27.01.2000). Sinon, la Commission ne se départit guère de formules rituelles se bornant à affirmer l'absence de toute preuve des allégations sur Echelon et ne pas avoir connaissance de violations du droit communautaire par des Etats membres (par ex. la réponse du commissaire BRITTAN donnée le 24 mars 1999 à la question écrite de Mr RAUTI, seulement publiée au *J.O.C.E.* C 341 du 29 novembre 1999, p. 94). Cf. aussi le communiqué de l'A.F.P. du 25.02.2000 : « <http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=3268> ».

(97) Déclaration du Commissaire LIIKANEN, compte-rendu intégral de la séance plénière du Parlement européen du 30 mars 2000.

(98) Arrêt *Khan c. Royaume Uni* du 12 mai 2000.

« (...) everything that has been conducted, or will be conducted, is in complete conformity with the United Kingdom law, with the United States law, and most importantly, is done with complete respect for and in complete conformity with the European Convention on Human Rights » (99).

En effet, si la réaffirmation de la conventionnalité du droit anglais vaut ce qu'elle vaut, l'insistance à souligner, dans une enceinte européenne, le respect du droit américain ne laisse pas de surprendre. Et quand bien même ces deux législations seraient-elles respectées, on ne voit guère en quoi cela peut concerner les personnes résidant en-dehors des territoires américain et britannique, puisque le droit international prohibe les écoutes téléphoniques extra-territoriales (100). Enfin, clamer que chaque écoute menée ou à venir est légale, *quod non*, ne revient-il pas à renforcer un peu plus la conviction que ces deux Etats y recourent bel et bien ?

Le Ministre de l'Intérieur portugais, dont le pays assurait la présidence du Conseil de l'Union au cours du premier semestre 2000, a toutefois déclaré ce même 30 mars qu'il n'y a

« pas de doute sur l'existence ou non d'un système d'interception des télécommunications »

et que

« ce qui est en question, c'est son utilisation ; nous n'avons pas d'informations précises sur les entreprises qui en auraient bénéficié ou souffert » (101).

Les Ministres de l'Intérieur et de la Justice des Quinze ont abordé le dossier Echelon (sous le libellé neutre « interception des télécommunications » lors du Conseil du 29 mai 2000) (102). En voici les conclusions :

« Le Conseil a eu un échange de vue sur les débats au Parlement européen concernant les interceptions de télécommunications en-dehors de tout cadre juridique.

Le Conseil réaffirme son attachement au respect des principes fondamentaux relatifs à la protection des droits de l'homme et des libertés fondamentales, tant pour les personnes physiques que morales, tels que reconnus par le Traité sur l'Union Européenne.

Si l'interception des télécommunications peut être un outil important dans la lutte contre la criminalité ou pour la défense de la sécurité nationale, elle ne peut en aucun cas être utilisée aux fins de procurer des avantages commerciaux.

Le Conseil a pris note de l'intention de la Commission de présenter prochainement des mesures appropriées dans la réalisation d'une société de l'information plus sûre.

(99) Intervention de Mr EVANS, compte-rendu intégral de la plénière du 30 mars 2000.

(100) Voyez *infra* à propos de la légalité défailante d'Echelon au regard de l'article 8 de la Convention européenne des droits de l'homme ainsi que dans la deuxième partie du présent article les motifs dispensant d'exercer avant de saisir la Cour de Strasbourg les voies de recours organisées par les Etats participant à Echelon.

(101) *Libération* 31.03.2000.

(102) *Libération* 03.04.2000.

Le Conseil demande à la Présidence de veiller à ce que les groupes de travail du Conseil concernés assurent le respect des principes énoncés ci-dessus et favorisent en particulier toute mesure de prévention et de protection contre l'utilisation abusive des nouvelles technologies » (103).

En langage diplomatique, cela doit signifier une reconnaissance implicite de l'existence d'Echelon (puisque tel est le débat au Parlement), concomitamment au refus d'une condamnation explicite (certains Gouvernements étant soupçonnés d'en faire partie); la condamnation discrète des interceptions de type commercial joute l'affirmation sur l'utilité des interceptions de sécurité. Autrement dit, le Conseil semble se refuser à réprouver tous les systèmes d'interception en soi, sans doute parce que d'autres qu'Echelon existent en Europe, en n'en fustigeant que certains usages (104).

15. La résolution sur Echelon du 11 avril 2000 de la Commission des Libertés du Parlement européen — Malgré les hésitations des instances communautaires, l'année 2000 a quand-même vu le Parlement adopter deux initiatives importantes concernant Echelon (105). Il s'agit, d'une part, de la résolution sur le système « Echelon » de la Commission des Libertés du 11 avril 2000 (106) et, d'autre part, de la constitution d'une commission temporaire décidée lors de la séance plénière du 5 juillet 2000.

La résolution « *Watson* » du 11 avril (du nom de son auteur qui préside également la Commission des Libertés) (107) a été bien accueillie par ses premiers commentateurs (108). Elle prend appui sur les auditions réalisées en février 2000 (dont celle, déterminante, de Duncan Campbell), les déclarations de l'ancien Directeur de la C.I.A. et la nécessité de renforcer partout les contrôles parlementaires. La résolution constate l'inadéquation des textes insuffisamment contraignants de l'O.C.D.E., de l'O.M.C. et de l'O.N.U. au niveau international.

(103) Communiqué de presse n° 8832/00 (Presse 183) relatif à la 2266^e rencontre du Conseil en date du 29 mai 2000 (disponible sur « <http://ue.eu.int/Newsroom/main.cfm?LANG=2> »).

(104) Or, ces conclusions ne peuvent en rien dispenser les systèmes d'interception de sécurité de respecter les textes internes, communautaires et internationaux protecteurs de la vie privée, d'une part, ni d'outrepasser la prohibition par le droit européen des droits de l'homme de tous les systèmes d'écoute « à caractère général et exploratoire » ou menant à des écoutes « par hasard », d'autre part.

(105) Toutes deux ont été discutées simultanément devant la Commission des Libertés du Parlement en même temps que se poursuivaient les auditions entamées les 22 et 23 février : procès-verbal de la réunion des 21 et 22 mars 2000, PE 232.268.

(106) Point 3 du procès-verbal de la réunion de la Commission des Libertés et des Droits des citoyens, de la Justice et des Affaires intérieures du 11 avril 2000, PE 285.918.

(107) La proposition de résolution sur le système « Echelon » de Mr WATSON (PE 285.911) a été déposée le 31 mars directement après les déclarations du Conseil et de la Commission lors de la séance plénière de la veille (pour le texte des amendements, voyez le document publié le 7 avril, PE 285.911/1-13). Aucun texte coordonné de la proposition et des amendements adoptés n'était disponible lors de la rédaction (cf. le procès-verbal de la réunion du 11 avril).

(108) D. CAMPBELL, « *Flaw in Human Rights Uncovered* », magazine en ligne *Telepolis*, 08.04.2000, « <http://www.heise.de/tp/english/inhalt/co/6724/1.html> »; J. THOREL, « Faut-il amender les droits de l'homme face aux risques de type Echelon ? », 13.04.2000, « <http://www.zdnet.fr/actu/tech/a0013919.html> ».

Mais la résolution « *Watson* » estime aussi dépassé le droit du Conseil de l'Europe (article 8 de la Convention européenne des droits de l'homme et Convention n° 108 de 1981 sur la protection des données personnelles) dont les garanties seraient en deçà de ce que les citoyens européens peuvent attendre car

« (les dispositions du Conseil de l'Europe) ne protègent pas des interceptions effectuées par un Etat membre dont ils ne sont pas ressortissants » (109).

Si cette affirmation doit être nuancée, ce texte met cependant clairement le doigt sur ce problème délicat que représente le caractère extra-territorial des écoutes téléphoniques menées dans le cadre d'Echelon et recommande que de telles écoutes soient au moins notifiées à l'Etat où se trouve la personne dont le message est intercepté (110).

L'autre point fondamental de la résolution du 11 avril 2000 réside dans la condamnation formelle du caractère général et exploratoire d'Echelon :

« toute interception systématique ne peut pas être considérée comme proportionnée, même si le but poursuivi est la lutte contre le crime international et, par conséquent, tout Etat membre qui recourrait à ce système devrait cesser de l'utiliser ».

16. La décision du 5 juillet 2000 d'installer une commission temporaire sur Echelon — Le choix entre commission d'enquête, habilitée à investiguer sur les responsabilités des Etats membres dans Echelon, et commission temporaire, aux pouvoirs moins étendus, a finalement été tranché au profit de cette dernière (111). Dès la Conférence des présidents du 13 avril 2000, il était déjà presque certain qu'aucune commission d'enquête ne serait constituée (112), en raison des réticences de la plus grande partie des eurodéputés allemands et britanniques et de la majorité des eurodéputés chrétiens-démocrates du groupe P.P.E. et socialistes du groupe P.S.E. (113).

Le mandat de la Commission temporaire sur Echelon décidée en séance plénière du 5 juillet 2000 (114) comporte 7 points (115) :

(109) Point J de la résolution « *Watson* » du 11 avril 2000.

(110) Les points F, G, L et M de la résolution « *Watson* » insistent à raison sur ce sujet. La notification n'est cependant valable au regard du droit international général que si elle est préalable et ménage ainsi la possibilité pour l'Etat où se trouve la personne qui fait l'objet de l'interception de marquer son accord ou non (cf. *infra*).

(111) Le choix avait déjà été évoqué en séance plénière du 30 mars. Le débat fut reporté le 13 avril (édition provisoire du procès-verbal de séance, point 3) et la question fit l'objet de querelles de procédure (intervention pour le groupe des Verts de Mr LANNØYE, édition provisoire du procès-verbal de la séance du 13 juin 2000, point 11). Il fut décidé en plénière du 14 juin (procès-verbal provisoire, point 2) d'attendre l'examen par la Conférence des Présidents de la demande de constitution de la commission temporaire.

(112) Voyez l'article J. THOREL, « Enquête allégée sur Echelon au Parlement européen », 14.4.2000, « <http://www.zdnet.fr/actu/tech/a0013938.html> ».

(113) J. van BUUREN, « Decision on inquiry on Echelon postponed for a week », *Telepolis*, 06.04.2000, « <http://www.heise.de/tp/english/inhalt/co/6714/1.html> ».

(114) Par 340 voix pour, 210 contre et 15 abstentions. La proposition de commission d'enquête a été rejetée par 137 pour, 407 contre et 20 abstentions. La commission temporaire, prési-

- vérifier l'existence du système d'interception des communications connu sous le nom d'Echelon;
- en vérifier la compatibilité avec le droit communautaire;
- regarder si les droits des citoyens européens sont protégés contre les activités des services secrets;
- analyser si le cryptage est suffisant pour protéger la vie privée;
- renforcer la prise de conscience des autorités européennes à l'égard de ces problèmes;
- vérifier si l'interception des communications au niveau mondial fait courir des risques à l'industrie européenne;
- et, le cas échéant, proposer des initiatives politiques et législatives.

Les critiques déplorent que le Parlement n'ait pas opté pour la commission d'enquête, mécanisme qui avait fait ses preuves dans la crise de la « vache folle » (116), d'autant que c'est cette institution qui a contribué à faire connaître les risques d'Echelon (117). L'argument de la mise à l'enquête sur Echelon par la DST française n'a donc pas résisté à une majorité qui estime que tous les grands Etats possèdent leurs systèmes d'interception, ce qui aurait risqué de détériorer les relations avec le Royaume Uni, sans compter que les officiels des pays concernés, tenus au secret-défense, n'auraient jamais témoigné (118).

Outre les divergences politiques doublées des divergences nationales qui habitent le Parlement européen sur Echelon, on dénote, à l'instar de ce qui se constate dans les enceintes parlementaires nationales, des attitudes presque schizophréniques en son sein. D'un côté, est décidée la constitution d'une commission temporaire, option minimaliste mais indicative malgré tout d'une avancée, sur un système de surveillance électronique globale. Mais de l'autre côté, fut approuvé en 1999 un rapport en vue de contraindre les opérateurs de mobilophonie à faciliter les écoutes en temps réels sur leurs réseaux (119). Les travaux menés par l'European Telecommunications Standards Institute (ETSI, organisme privé de normalisation regroupant les principaux opérateurs) ont abouti en mars 2000 à un document en passe d'être soumis aux autorités nationales de régulation des télécommunications, lequel a été qualifié de « *sorte de vade-mecum technique de l'écoute moderne* » (120).

dée par Mr COELHO, a déjà programmé des réunions du 5 septembre au 23 novembre 2000 (« <http://www.europarl.eu.int/tempcom/echelon/fr/agenda.htm> »).

(115) Décision du 5 juillet 2000, B5-0594/2000.

(116) *L'Echo* 06.07.2000.

(117) *Libération* 06.07.2000.

(118) *La Libre Belgique* 06.07.2000.

(119) Ph. ASTOR, « Le Parlement européen vote pour l'écoute des réseaux », 15.05.1999, « <http://www.zdnet.fr/actu/inte/a0009329.html> ».

(120) Le document de l'ETSI, particulièrement abscons, s'intitule *Intelligent Networks (IN) : Lawful Interception*. Il est téléchargeable en consultant l'article de J. THOREL, « Les réseaux européens sur écoute », 21.06.2000, « <http://www.zdnet.fr/actu/tech/secu/a0014766.html> » ou par l'adresse « <http://www.zdnet.fr/actu/etsi.pdf> ». Une harmonisation des procédures techniques est

Toujours est-il que l'état d'avancement et le degré d'investigation d'une commission aux moyens juridiques limités conditionneront tant les travaux communautaires que nationaux. Le mandat de la commission temporaire est, entre autres, de vérifier la compatibilité d'Echelon avec le droit communautaire. Outre les Directives 95/46/CE et 97/66/CE sur la protection des données personnelles, il concerne aussi l'article 6, § 2, du Traité sur l'Union européenne qui érige en principes généraux du droit communautaire la Convention européenne des droits de l'homme. Une Convention qui, interprétée par une jurisprudence résolument évolutive, est particulièrement adaptée à l'analyse et la contestation d'Echelon.

2. La Convention européenne des droits de l'homme est « technologiquement pertinente »

17. Les débats devant le Parlement européen ont soulevé certains doutes quant à l'utilité de la Convention européenne des droits de l'homme. Si la question doit être posée, l'exhumation d'une décision oubliée et longuement motivée de l'ancienne Commission européenne des droits de l'homme montre qu'une partie d'Echelon a déjà été analysée à Strasbourg, premier gage d'utilité de la Convention (I.A.2.a.). Mais c'est surtout une jurisprudence résolument protectrice de la vie privée, et remontant à 1978 déjà, qui permet d'invoquer la protection de l'article 8 de la Convention, lequel garantit le droit au respect de la vie privée, qui ouvre les perspectives les plus intéressantes. Les conversations téléphoniques et, par extension, tout message transitant par toute forme de technologie sont protégés par la Convention. La jurisprudence imposante qu'elle a suscitée inspire d'ailleurs tant le droit du Conseil de l'Europe que celui de l'Union européenne (I.A.2.b.).

a) De quelques analyses approximatives de la Convention devant le Parlement européen au sujet d'Echelon

18. Replacer les règles sur les écoutes téléphoniques dans le contexte de la Convention prise dans son ensemble — La résolution

souhaitable si les interceptions ne peuvent être opérées par chaque État que dans le respect de sa législation. Mais l'harmonisation permettra les écoutes extra-frontalières, mécanisme fort sujet à caution comme cela sera abordé plus loin. Elle n'offre que peu de garanties contre des usages extra-légaux. Cette harmonisation montre au demeurant à ceux qui douteraient de la faisabilité technique d'Echelon qu'elle est bien réalisable. A noter enfin que ceci résulte des pressions américaines qui ont eu toutes les occasions d'être exercées lors des séminaires conjoints qui se tenaient au moins jusque 1997 entre services américains, services des 15 et de quelques autres pays, dont les parties à l'accord UKUSA. On peut en outre se demander quelle protection juridique offre un texte non contraignant qui encourage une harmonisation qui, elle, va se concrétiser incessamment (remarque judicieuse de Mr FLORIO, rapporteur de la Commission juridique et des droits des citoyens, dont l'avis du 25 mars 1999 est annexé au rapport de Mr SCHMID sur le projet de résolution du Conseil relative à l'interception légale des télécommunications compte tenu des nouvelles technologies, 23 avril 1999, PE 229.986/déf., p. 9. Voyez aussi *infra*).

« *Watson* » du 11 avril 2000 condamne à juste titre les écoutes systématiques et les interceptions extra-territoriales sans notification. Elle présente cependant une lacune. Si elle estime que les Etats qui participent à une structure semblable à Echelon doivent immédiatement cesser de tels agissements, la résolution n'aborde toutefois pas l'hypothèse de la participation passive (accueil par un Etat membre d'une base d'interception exploitée par les services d'un autre Etat, tiers ou non). Dans ce cas aussi, la Convention européenne des droits de l'homme, qui met à charge de ses signataires des obligations de vigilance (comme celle de ne pas mettre leur territoire à disposition pour faciliter la violation du droit au respect de la vie privée), impose la cessation de cette participation illicite. Aussi, les réserves émises par la résolution « *Watson* » sur l'efficacité de la Convention européenne des droits de l'homme ne paraissent-elles pas pertinentes (121). Il convient, en effet, de replacer la jurisprudence de la Cour de Strasbourg sur les écoutes téléphoniques dans le système de la Convention pris dans son ensemble.

Les mêmes remarques doivent être formulées à l'égard du rapport du professeur Elliott sur « *The legality of the interception of electronic communications* » (déposé en octobre 1999, il compose l'une des cinq parties du rapport actuellement analysé par le Parlement Européen). Il met bien à jour diverses convergences juridiques : protection contre les écoutes illégales par l'article 8 de la Convention ainsi que les droits internes sur les libertés publiques ; législation autorisant des écoutes dans la plupart des Etats membres ; à l'instar des Etats Unis et de l'Australie, recommandations aux compagnies de télécommunications pour faciliter les écoutes légales ; législation de la plupart des Etats membres requérant des opérateurs la protection des communications contre les écoutes illégales ; autorisation, sauf en France, des systèmes de cryptage pour sécuriser le commerce électronique... Mais le rapport « *Elliott* » s'achève en se limitant à poser le problème de l'interception des communications par un Etat tiers, sans apporter aucun élément de solution (122).

L'objet de la présente étude est dès lors de dépasser la réserve sur l'efficacité de la Convention européenne des droits de l'homme qu'a émise la résolution « *Watson* » et le constat de carence du rapport « *Elliott* ». Car l'article 8 de la Convention ne se contente pas de garantir le droit au respect de la vie privée et de la correspondance. C'est également une norme permettant de contester effectivement la participation par des Etats membres de

(121) Le souci poursuivi de promouvoir des textes communautaires encore plus protecteurs de la vie privée mérite évidemment tous les égards. Sur les obligations de vigilance, *infra* le n° 49 à propos de l'article 13 de la Convention.

(122) Le résumé du rapport « *Elliott* » affirme que « *there do not appear to be adequate legal processes to protect privacy against unlawful interception, either by foreign governments or by non-governmental bodies* » (p 1). La conclusion, faisant suite au constat de diverses convergences, que « *the position is less clear with regard to interception by foreign powers, particularly because of the fundamental technological change from switched circuits to packet switching* » (p 13).

l'Union Européenne, lesquels sont tous Parties à la Convention, au programme de surveillance électronique globale Echelon (123). L'application extra-territoriale d'actes de contrainte comme les écoutes téléphoniques pose ainsi de sérieuses questions de validité au regard du droit international général et de la Convention.

19. Une décision oubliée d'irrecevabilité de la Commission européenne des droits de l'homme avait trait à Echelon... — La Convention européenne des droits de l'homme ne peut nullement s'interpréter comme prohibant l'existence de services secrets; le bon fonctionnement d'une société démocratique fondée sur la primauté du droit peut même l'exiger. Un État peut ainsi se protéger des individus et des groupes, voire des autres États, qui tentent de porter atteinte aux valeurs essentielles d'une société démocratique, afin de garantir sa sécurité nationale, son intégrité territoriale ou la sûreté publique sur son territoire (124). Encore faut-il que les activités des services secrets respectent les règles générales du droit international public, en particulier celles relatives à la souveraineté territoriale, ainsi que, bien entendu, la Convention lorsque l'Etat en cause y est partie.

Les écoutes et interceptions électroniques sont des faits au regard du droit international, qu'elles résultent d'une ou plusieurs lois internes ou d'une convention internationale ou encore d'un mandat judiciaire ou d'activités purement administratives. Comme la Cour européenne des droits de l'homme l'a posé à plusieurs reprises, peu importe le type d'autorité à laquelle se trouve imputé le fait qui constituerait un manquement à une obligation internationale puisque, devant elle, c'est la responsabilité de l'Etat qui se trouve mise en cause (125). Même si par son fonctionnement international, transfrontalier, voire extra-européen, d'une part, et ses caractères secret et systématique, d'autre part, Echelon est d'analyse difficile, cinquante années de jurisprudence des organes de la Convention européenne des droits de l'homme et des juridictions nationales permettent aujourd'hui de contester la validité.

La contestation des écoutes et interceptions électroniques au regard de l'article 8 de la Convention européenne des droits de l'homme n'est nullement théorique. Bien au contraire.

Aucune enquête officielle ou journalistique ne paraît en effet avoir tenu compte jusqu'à présent de ce que la Commission européenne des droits de l'homme a eu à connaître, dans au moins une décision publiée, d'une

(123) Les principes exposés ici demeurent pleinement pertinents pour contester les autres programmes de surveillance électronique globale. Leur application serait même facilitée quand un État procède seul *urbi et orbi* à des écoutes en-dehors de tout arrangement « transnational ».

(124) Arrêt *Vereniging Weekblad 'Bluf!' c. Pays-Bas* du 9 février 1995, § 35. En dernier lieu, l'arrêt *Rotaru c. Roumanie* du 4 mai 2000, § 47.

(125) Arrêt *Lingens c. Autriche* du 8 juillet 1986, § 46.

requête relative à l'interception de téléfax envoyés entre un syndicaliste anglais et des syndicats d'Europe de l'Est. Rien d'extraordinaire là-dedans, d'autant que la requête fut déclarée irrecevable pour défaut de fondement (ce que le Royaume Uni ne manquerait pas de soulever pour attester de la conformité de son droit interne). Si ce n'est peut-être que les services anglais auraient fait en l'occurrence usage d'un logiciel appelé ... « Dictionary » (126), soit celui qui ferait tourner Echelon. Cette mention dans une décision officiellement publiée par une instance internationale comme la Commission européenne des droits de l'homme, qui ne soupçonnait peut-être pas de quoi il retournait exactement, est sans doute un des indices les plus probants sur le plan juridique de l'existence d'Echelon.

Seul les cas de l'Allemagne (base US de Bad Aibling (127) et du Royaume Uni (base UK-US de Menwith Hill et bases UK de Morwenstowe et Cheltenham) sont abordés, ci-après, de manière plus approfondie en raison du nombre de sources concordantes quant à l'implantation de stations d'interception sur leur sol. Mais il va sans dire que s'il s'avérait que d'autres pays parties à la Convention européenne des droits de l'homme jouaient également un rôle, fût-ce passif, dans le cadre d'Echelon, les principes exposés dans le présent article leurs seraient tout autant applicables.

b) *Une jurisprudence strasbourgeoise résolument évolutive sur les ingérences dans la vie privée perpétrées à l'aide des nouvelles technologies*

20. Depuis 1978, les écoutes téléphoniques sont considérées comme des ingérences dans le droit au respect de la vie privée et de la correspondance alors que le texte de l'article 8 de la Convention n'en parle pas — L'article 8 de la Convention européenne des droits de l'homme garantit le droit au respect de la vie privée :

« § 1^{er} — Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

(126) Décision du 27 juin 1994 dans l'affaire *Christie contre Royaume Uni*, req. n° 21482/93, D.R. 78-A, p. 119. La Commission européenne des droits de l'homme mentionnait en effet ceci dans le relevé des faits de la cause : « *In or about July 1991, it came to the attention of the applicant, in the context of a Granada television documentary 'Defending the realm', that telexes addressed to himself from East European trade unions were being routinely intercepted by GCHQ (Government Communications Headquarters) which is the United Kingdom's central intelligence-gathering centre. Information from those telexes had been collated and reported to other government agencies. The evidence for these allegations was provided anonymously by a former GCHQ employee, who also stated that at a particular address in London all telexes passing in and out of London were intercepted and fed into a programme known as 'the Dictionary', which picked out key names and words. He stated that 'the Dictionary' was monitored by carefully vetted British Telecom employees to give the impression that GCHQ was not carrying out the interception and that warrants were not obtained for this activity.* »

(127) En ce qui concerne par ailleurs la coopération éventuelle du BND allemand avec les services américains, voyez l'article de W. MADSEN, « Crypto AG : The NSA's Trojan Whore ? » sur le site du magazine *Covert Action Quarterly* « <http://mediafilter.org/CAQ/caq63/caq63madsen.html> ».

§ 2 — *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et liberté d'autrui.*

La Cour européenne des droits de l'homme a su s'adapter aux réalités technologiques en posant, depuis 1978, que les écoutes téléphoniques constituaient des ingérences dans le droit au respect de la vie privée et de la correspondance. Le Conseil de l'Europe et les Communautés Européennes s'en sont inspirés depuis lors dans tous les instruments (conventions, directives, résolutions,...) de protection de la vie privée qu'il s'agisse de la réglementation des banques de données, des écoutes par la police, des télécommunications ou encore d'Internet, toutes ces pratiques étant constitutives d'ingérences potentielles dans les droits fondamentaux. Toute écoute, toute interception, tout stockage, tout traitement de messages transmis par une voie électronique quelconque constituent en effet autant d'ingérences dans le droit eu respect de la vie privée. Celles-ci ne sont compatibles avec la Convention que si trois conditions examinées dans la deuxième partie sont cumulativement remplies.

Car le caractère dynamique de l'interprétation des termes autonomes de la Convention par les organes de celle-ci a très tôt permis de qualifier les écoutes téléphoniques d'ingérences dans le droit au respect de la vie privée et de la correspondance (128). En effet, la décision de principe dans le domaine des écoutes téléphoniques, rendue en 1978 dans l'affaire *Klass contre Allemagne*, a bien précisé que

« quoique le paragraphe 1 de l'article-8 ne mentionne pas les conversations téléphoniques (...), elles se trouvent comprises dans les notions de 'vie privée' et de 'correspondance' visées par ce texte ».

De surcroît,

« manifestement, chacune des mesures de surveillance permises, une fois exécutée contre un individu donné, entraînerait une ingérence d'une autorité publique dans l'exercice du droit de l'intéressé au respect de sa vie privée et familiale et de sa correspondance. De plus, la législation elle-même crée par sa simple existence, pour tous ceux auxquels on pourrait l'appliquer, une menace de surveillance entravant forcément la liberté de communication entre usagers des services des postes et télécommunications et constituant par là une 'ingérence d'une autorité publique' dans l'exercice du droit des requérants au respect de leur vie privée et familiale ainsi que de leur correspondance » (129).

(128) De manière générale, voyez les actes du colloque des 13 et 14 mars 1998 organisé par l'Institut de droit européen des droits de l'homme de l'Université de Montpellier, F. SUDRE (dir.), *L'interprétation de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant et Nemesis, 1998.

(129) Arrêt *Klass c. Allemagne* du 4 juillet 1978, § 41.

21. Caractéristique de l'Etat policier, l'écoute n'est tolérée qu'individuellement et seulement si elle est strictement nécessaire dans une société démocratique — La Cour européenne des droits de l'homme a rappelé à plusieurs reprises que le terme « vie privée » ne doit pas être interprété de manière restrictive dans la mesure où

« le respect de la vie privée englobe le droit pour l'individu de nouer et de développer des relations avec ses semblables ».

En outre,

« aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de 'vie privée' » (130).

Il ne fait dès lors aucun doute que les écoutes, interceptions, relevés, traitements ou stockages de messages délivrés par voie de téléphonie fixe ou mobile, le courrier électronique, les télex et téléfax sont également couverts par l'article 8, d'une part, et que chaque écoute, interception, relevé, traitement ou stockage constituent également à chaque fois une ingérence distincte, d'autre part. Ce qui signifie, en d'autres termes, que chaque ingérence, prise isolément, doit être conforme à l'article 8. Or,

« l'existence (...) de lois et pratiques autorisant et instaurant un système de surveillance secrète des communications constitue en soi une 'ingérence' » (131).

Les conditions de la conformité des écoutes avec l'article 8 ont été exposées avec une force sans pareille dans l'arrêt *Klass* toujours, jalons essentiel de la définition de ce qu'est une société démocratique (132) :

« La principale question qui se pose en l'occurrence sur le terrain de l'article 8 consiste à savoir si les termes du paragraphe 2 justifient l'ingérence ainsi constatée. Ménageant une exception à un droit garanti par la Convention, ce paragraphe appelle une interprétation étroite. Caractéristique de l'Etat policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques » (133).

Peu importe qu'il y ait ou non utilisation ultérieure des enregistrements effectués (134).

Peu importe aussi le contenu effectif de la communication interceptée. Comme la Commission européenne des droits de l'homme l'a affirmé dans un rapport du 2 septembre 1992,

(130) Voyez en dernier lieu l'arrêt *Amann c. Suisse* du 16 février 2000, § 65. F. SUDRE a pu parler des « Aléas de la notion de 'vie privée' dans la jurisprudence de la Cour européenne des droits de l'homme » (in *Mélanges L.E. Pettiti*, Bruxelles, Bruylant, 1998, pp. 687-706) mais son propos ne critiquait pas les arrêts sur les écoutes téléphoniques.

(131) Une seule écoute téléphonique suffit pour qu'il y ait ingérence comme la Cour l'a jugé dans son arrêt *Malone c. Royaume-Uni* du 27 juin 1984, § 64.

(132) F. OST, « Le concept de 'démocratie' dans la jurisprudence de la Cour européenne des droits de l'homme », *Journ. Proc.*, n° 124, 4 mars 1988, pp. 13-19.

(133) Arrêt *Klass*, § 42. C'est nous qui soulignons.

(134) Arrêt *Kopp c. Suisse* du 25 mars 1998, § 53.

« les conversations téléphoniques, tout comme la correspondance par lettres, sont en principe confidentielles dans tous États de droit et cette confidentialité de principe dont elles sont entourées les place dans le domaine de la sphère privée. Le caractère privé d'une conversation téléphonique ne disparaît pas du seul fait que le contenu de ladite conversation concerne ou peut intéresser le domaine public. Si le domaine protégé par l'article 8 était limité aux seuls aspects de la vie privée, desquels se désintéresse la puissance publique, cette disposition serait, en grande partie, vidée de sa substance. De plus, la décision de procéder à des écoutes téléphoniques ou à l'enregistrement de conversations téléphoniques est nécessairement prise avant que le contenu de la conversation soit connu avec certitude » (135).

Peu importe également que les appels interceptés émanent ou soient en direction du domicile ou de locaux professionnels : l'article 8 de la Convention leur est à tous applicable (136). Il en va de même si les écoutes à l'encontre d'une personne sont effectuées sur la ligne d'un tiers (137).

22. Une interprétation large de la vie privée qui inspire directement tout le droit du Conseil de l'Europe — Selon une jurisprudence européenne désormais bien établie depuis l'arrêt *Klass* de 1978 jusqu'aux tout récents arrêts *Amann contre Suisse* du 16 février 2000 et *Khan contre Royaume Uni* du 12 mai 2000, ces principes jurisprudentiels s'appliquent aussi bien aux écoutes judiciaires qu'aux écoutes administratives même si certaines particularités sont inhérentes à ces dernières (138).

L'ensemble de ces principes est également applicable à la mémorisation de données relatives à la « vie privée » (139), ainsi qu'aux modes d'enquête comme la prise d'empreintes digitales, la fouille d'une personne, le fait de poser des questions sur la vie privée, la prise de photos ou la conservation d'un procès-verbal d'audition (140).

Il est d'ailleurs très significatif que bon nombre d'instruments européens se réfèrent expressément à l'article 8 de la Convention européenne des droits de l'homme pour indiquer aux États comment réglementer les télécommunications en conformité avec cette disposition (141). Le meilleur

(135) Rapport cité par P. WACHSMANN, « Les écoutes téléphoniques », obs. sous l'arrêt *A. c. France* du 23 novembre 1993, *R.T.D.H.* 1994, pp. 582-583.

(136) Arrêt *Halford c. Royaume Uni* du 25 juin 1997, § 44; arrêt *Kopp c. Suisse* du 25 mars 1998, § 50.

(137) Arrêt *Lambert c. France* du 24 août 1998, § 21.

(138) G. COHEN-JONATHAN, « Les écoutes téléphoniques », in. *Mélanges G.J. Wiarda*, Karl Heymans Verlag, Cologne, 1988, p. 100.

(139) Arrêt *Leander c. Suède* du 26 mars 1987, § 48; arrêt *Amann c. Suisse* du 16 février 2000, § 65.

(140) Rapport de la Commission du 18 mars 1981 dans l'affaire *Mac Veigh, O'Neill et Evans c. Royaume Uni*, D.R. 25, p. 15, § 224. Si la prise de photos par la police au cours d'une manifestation se déroulant dans la rue n'est pas constitutive d'ingérence, l'interrogatoire sur l'identité et l'enregistrement de données y relatives qui peuvent s'ensuivre constituent par contre une ingérence (Comm.eur.d.h., rapport du 19 mai 1994, req. n° 15225/89, *Friedl c. Autriche*, « <http://www.dhcour.coe.fr/Hudoc1doc/herrep/sift/305.txt> », §§ 49 et 52).

(141) C'est le cas du Préambule de la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ainsi que de toutes les Recommandations du Comité des Ministres du Conseil de l'Europe

exemple en est la Recommandation n° R (95)4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, adoptée le 7 février 1995 par le Comité des Ministres du Conseil de l'Europe. Son exposé des motifs est on ne peut plus explicite :

« La protection établie dans cette disposition s'étend également à la garantie du secret de la correspondance. Pour la Cour européenne des droits de l'homme, cette garantie doit s'appliquer aux conversations téléphoniques tout autant qu'au courrier. Le souhait de la Cour de rendre la Convention européenne des droits de l'homme technologiquement pertinente doit donc être considéré comme autorisant de placer la gamme complète des services de télécommunication qui permettent la communication ou la correspondance entre abonnés ou les utilisateurs sous la protection énoncée à l'article 8 de la Convention européenne des droits de l'homme » (142).

L'interpénétration entre les systèmes européens de protection de la vie privée n'est plus à démontrer. Si la Convention du Conseil de l'Europe de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel s'inspire explicitement de l'article 8 de la Convention européenne des droits de l'homme, la Cour s'inspire à son tour de cette Convention de 1981 pour interpréter l'article 8 (143).

23. Une interprétation large qui sous-tend aussi tout le droit communautaire et qui est également celle du Comité des droits de l'homme — Quant aux directives communautaires sur le traitement des données à caractère personnel, elles se réfèrent également au droit du Conseil de l'Europe, en ce compris l'article 8 de la Convention européenne des droits de l'homme, comme sources inspirant directement la protection qu'elles visent à offrir à la vie privée (144).

qui tendent à en préciser la portée (en dernier lieu la Recommandation n° R (99) 5 du 23 février 1999, qui comporte les lignes directrices pour la protection de la vie privée sur Internet; pour une liste exhaustive de ces recommandations, cons. le site du Conseil de l'Europe à la page <http://www.coe.fr/dataprotection/fdocs.htm> »).

(142) Exposé des motifs de la Recommandation n° R (95)4 du Comité des Ministres du Conseil de l'Europe, point 29 (c'est nous qui soulignons). Le développement des lignes RNIS (réseau numérique à intégration de services) a poussé le Comité des Ministres à ne pas limiter son approche à la téléphonie vocale, pour englober également la transmission de textes ou d'images par fax, vidéotexte interactif ou télémétrie.

(143) En dernier lieu, l'arrêt *Rotaru c. Roumanie* du 4 mai 2000, § 43.

(144) Le point 10 des considérants préliminaires 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 (*J.O.C.E.* n° L 281 du 23.11.1995), renvoie tout à la fois aux droits nationaux, à l'article 8 de la Convention et aux principes généraux du droit communautaire en assignant pour objectif à l'Union un niveau encore plus élevé de protection en supprimant les disparités dans l'organisation de celle-ci. Consultez aussi la Directive 97/66/CE du Parlement 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 (*J.O.C.E.* n° L 024 du 30.01.1998).

Les nouvelles propositions de la Commission européenne visant à tenir compte des évolutions technologiques dans le secteur des communications électroniques ne s'écartent évidemment pas de cette ligne de conduite (145).

Le Comité des droits de l'homme de l'O.N.U., s'il n'a pas encore eu, à notre connaissance, à connaître d'affaires de ce genre, s'est néanmoins préoccupé dès 1988, à l'aube de la croissance exponentielle des télécommunications et des nouvelles technologies, du problème des écoutes téléphoniques. L'observation générale n° 16 du Comité qui portait sur l'article 17 du Pacte international relatif aux droits civils et politiques, disposition qui garantit également le droit au respect de la vie privée et de la correspondance, affirme notamment que

« Même pour ce qui est des immixtions qui sont conformes au Pacte, une loi pertinente doit préciser dans le détail les cas précis dans lesquels elles peuvent être autorisées. La décision de procéder à des immixtions autorisées doit être prise par l'autorité désignée par la loi, et cas par cas. Le respect de l'article 17 exige que l'intégrité et le caractère confidentiel de la correspondance soient garantis en droit et en fait. La correspondance doit être remise au destinataire, sans interception, sans être ouverte, et sans qu'il en soit pris autrement connaissance ».

Le Comité va même très loin en n'hésitant pas à poursuivre en ces termes :

« la surveillance, par des moyens électroniques ou autres, l'interception des communications téléphoniques, télégraphiques ou autres, l'écoute et l'enregistrement des conversations devrait être interdit » (146).

Les pays membres de l'Union européenne ont tous adhéré à la Convention européenne comme au Pacte international. Ceux qui participent à Echelon ne peuvent dès lors ignorer que chaque écoute constitue en soi une ingérence qui ne se trouve en conformité avec l'article 8 que si sont simultanément réunies les trois conditions cumulatives de légalité, de légitimité et de nécessité dans une société démocratique, ces conditions s'appliquant tant au fond même des écoutes qu'aux garanties procédurales qu'elles requièrent.

B. — *Protection de la vie privée et droit à un recours effectif contre la surveillance électronique secrète*

24. La Convention européenne des droits de l'homme comporte deux dispositions fondamentales avec lesquelles Echelon se trouve vraisemblable-

(145) Point 2 des considérations préliminaires de la proposition, par la Commission, d'une Directive du Parlement et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, COM(2000) 385, 12 juillet 2000, p. 10.

(146) C.D.H., *Le droit au respect de la vie privée, de la famille, du domicile et de la correspondance, et le droit d'être protégé contre les atteintes à l'honneur et à la réputation (art. 17)*, Observation générale n° 16 du 8 avril 1984, § 8. Consultable sur le site du Haut Commissariat aux Droits de l'Homme de l'O.N.U. à l'adresse : « <http://www.unchr.ch/tbs/doc.nsf> ». Ce site permet aussi l'accès à la jurisprudence récente du Comité.

ment en contrariété. L'article 8 dont il vient d'être question du principe et dont les conditions de mise en œuvre sont décrites maintenant (I.B.1.) et l'article 13 qui garantit le droit à un recours effectif devant une instance nationale en cas d'atteinte à un droit garanti par la Convention (I.B.2.). La jurisprudence déjà ancienne de la Commission et de la Cour européennes des droits de l'homme est particulièrement confortée par des évolutions récentes qui en assoient l'effectivité.

1. Les conditions de validité des écoutes téléphoniques et de leurs dérivés modernes au regard de l'article 8 de la Convention

25. Nous sommes au cœur même du débat. L'article 8 de la Convention, pour être respecté, doit voir les ingérences dans la vie privée être conformes à trois conditions cumulatives. Première de ces conditions : la légalité de l'ingérence qui, dans le cas d'Echelon, ferait défaut à plusieurs titres. Quelle est la loi le régissant ? Peut-elle, si elle existe, être appliquée en-dehors du territoire des Etats qui y participent ? Et si c'est le cas, peut-elle aller à l'encontre des droits nationaux qui, comme en Belgique, prohibent les écoutes administratives ? De toute façon, cette loi serait-elle suffisamment prévisible dans ses conséquences pour toutes les personnes résidant sur le territoire du Conseil de l'Europe ? Serait-elle même suffisamment accessible ? Autant de questions de « légalité » qui paraissent déjà faire défaut (I.B.1.a.).

Echelon peut se révéler également contraire au principe de la légitimité requise des ingérences dans la vie privée. La Cour européenne des droits de l'homme commence à envisager le contrôle de la légitimité des motifs de sécurité nationale ou de bien-être économique du pays invoqués à l'appui des activités des services de renseignement, ce qu'elle se refusait à faire il y a peu encore (I.B.1.b.).

Mais Echelon ne résisterait guère non plus au troisième contrôle, celui de sa nécessité dans une société démocratique. D'abord parce que son fonctionnement est exploratoire et général, ensuite parce qu'une ingérence dans la vie privée, telle une écoute téléphonique, n'est réputée proportionnée à l'objectif poursuivi par le service de renseignement que si elle peut être contestée au terme d'une procédure « équitable » (I.B.1.c.).

a) *Une légalité douteuse : les manquements à la qualité de la « loi », son absence et les débordements territoriaux de celle-ci*

1. L'exigence de l'existence d'une « loi »

a. Echelon contre le principe même de l'existence d'une « loi »

26. Il faut qu'existe une « loi » régissant Echelon : une exigence évidente mais déjà problématique — Avant toute chose, une ingérence

dans un droit garanti doit, pour être « prévue par la loi » au sens de la Convention, avoir une base en droit interne (147) et être conforme aux dispositions que prévoient le droit interne (148). Cette première exigence, élémentaire, renvoie aux multiples droits internes applicables aux écoutes qu'elles soient administratives ou judiciaires (149).

Le droit international, même complexe et technique comme celui des télécommunications, peut tenir lieu de « loi » quand il est suffisamment accessible, clair et précis (150). Dans les pays de *common law*, le droit non écrit joue aussi le rôle de la « loi » (151). De même, la jurisprudence peut passer pour remplir la condition de légalité dans les systèmes juridiques de droit écrit : la « loi » est alors le texte en vigueur tel qu'interprété par les juridictions compétentes « *en ayant égard, au besoin, à des données techniques nouvelles* » (152).

De manière générale, la Cour européenne des droits de l'homme s'attarde rarement sur la question de l'existence d'une « loi » dans la mesure où elle estime ne pas avoir à se substituer aux juridictions internes en ce qui concerne les constatations de conformité au droit interne applicable (153). Encore que lorsqu'une décision judiciaire n'autorise la saisie du courrier d'un failli par le liquidateur que pour un terme donné, la rétention de sa

(147) Arrêt *Sunday Times c. Royaume Uni* du 26 avril 1979, § 47.

(148) Arrêt *Barthold c. Allemagne* du 25 mars 1985, § 48. De manière générale : F. MATSCHER, « Dans quelle mesure une violation du droit national entraîne-t-elle une violation de la Convention ? », in *Mélanges L.E. Pettiti*, Bruxelles, Bruylant, 1998, pp. 579-592, qui n'aborde cependant pas la question de savoir si une violation du droit international pourrait violer la Convention. Le Comité des droits de l'homme ne vérifie aussi la conformité au droit interne que s'il est manifeste qu'il y a eu appréciation arbitraire ou déni de justice flagrant (décision du 25 mars 1999, com. n° 844/1998, *Petkov c. Bulgarie*, point 4.2; décision du 15 mars 2000, com. n° 891/1999, *Tamihere c. Nouvelle-Zélande*, point 4.4).

(149) Une telle analyse des droits internes peut certes s'avérer édifiante. Il n'est toutefois pas recouru ici aux méthodes du droit comparé pour les raisons évoquées plus haut, d'autant plus que se posent des questions tenant aux conflits de lois applicables. Voyez cependant *infra* à propos de la primauté qu'il convient de réserver à la règle de droit interne quand elle est plus favorable aux droits garantis par la Convention que celle-ci.

(150) C'est par exemple le cas des conventions de l'Union Internationale des Télécommunications surtout quand elles sont d'abord applicables à des professionnels : arrêt *Groppera Radio AG et autres c. Suisse* du 28 mars 1990, § 68. Également, à propos des traités internationaux, la décision de la Commission du 15 mars 1984, *A. Association et H. c. Autriche*, req. n° 9905/82, D.R. 36, p. 187.

(151) Arrêt *Sunday Times c. Royaume Uni* du 26 avril 1979, § 47.

(152) Arrêt *Huwig c. France* du 24 avril 1990, § 28; arrêt *Kruslin c. France* du 24 avril 1990, § 29.

(153) Dans l'affaire *Klass*, les lois régulièrement adoptées par le Parlement et modifiées après intervention de la Cour constitutionnelle remplissaient assurément cette exigence (§ 43 de l'arrêt). Si l'exercice du contrôle de conformité au droit interne en tant que composante de la « légalité » de l'acte querellé au regard de la Convention est demeuré exceptionnel dans la jurisprudence de la Cour, celle-ci vient cependant de condamner la France en raison du rejet d'un pourvoi par la Cour de cassation, rejet motivé par une erreur manifeste d'appréciation des faits de la cause (arrêt *Dulaurans c. France* du 21 mars 2000).

correspondance postérieurement à ce délai ne peut passer pour être conforme à la « loi » et entraîne donc violation de l'article 8 (154).

Néanmoins, la Cour a déjà directement constaté la violation de l'article 8 en raison de l'absence de toute base en droit interne d'écoutes téléphoniques auxquelles un haut fonctionnaire de police avait procédé (155). Il en alla de même à propos de l'absence de toute réglementation de l'interception, au détriment d'un fonctionnaire de police, d'appels transmis sur des systèmes de télécommunications indépendants du réseau public, ce qui valut au Royaume Uni une condamnation (156).

Le programme Echelon pose déjà problème à ce tout premier stade de l'analyse de sa conformité avec l'article 8 de la Convention. On pressent vaguement qu'il repose en partie sur l'accord UKUSA qui fonde la collaboration en matière de renseignement entre le Royaume Uni et les États Unis et son extension à la Nouvelle Zélande, au Canada et à l'Australie. Mais cet accord règle-t-il les écoutes proprement dites ? L'Allemagne ou le Japon qui accueillent sur leur territoire des relais et des stations d'écoutes sont-ils parties prenantes à d'autres titres ? Un droit national est-il appliqué plus particulièrement ? Autant de questions qui portent donc déjà sur l'existence même d'une « loi » applicable.

b. *Le domaine de validité de la « loi » : Echelon contre l'interdiction des actes de contrainte à portée extra-territoriale*

27. Quel « territoire » recouvrent les droits de l'homme face à une technologie en perpétuel perfectionnement ? — Un des problèmes les plus importants, quoique peu étudié, qui se pose dans le droit moderne des droits de l'homme tient dans la délimitation de ce que le professeur Emmanuel Decaux appelle « *le territoire des droits de l'homme* » (157). Il est certain à l'heure actuelle que ce problème trouve son pendant dans celui, tout aussi fondamental, de la détermination de la législation pénale applicable à Internet et aux nouvelles technologies vu les multiples possibilités de conflits entre les divers droits applicables. Internet, pour peu que chacun puisse y avoir accès est un merveilleux outil de communication et de connaissance. Mais l'usage des nouvelles technologies de l'information doit évidemment

(154) Arrêt *Foxley c. Royaume Uni* du 20 juin 2000, § 35.

(155) Arrêt *A. c. France* du 23 novembre 1993, § 38. Cet arrêt est également très intéressant dans la mesure où il établit la responsabilité de la France pour des actes *ultra vires* commis par un officier supérieur de police.

(156) Arrêt *Halford c. Royaume Uni* du 25 juin 1997, § 50. Il faut souligner que l' *Interception of Communications Act* de 1985, qui ne réglementait pas les écoutes contestées dans cette affaire, avait été adopté par le Royaume Uni à la suite de sa condamnation dans l'affaire *Malone*. L'arrêt *Halford* fut à son tour une des justifications de l'adoption du *Regulation of Investigatory Powers Act 2000*.

(157) Selon le titre éponyme de l'étude parue dans les *Mélanges M.A. Eissen*, Bruxelles et Paris, Bruylant et L.G.D.J., 1995, p. 65.

être réglementé, en particulier quand elles servent de support à des comportements délictuels (158).

L'existence du programme Echelon, comme celle de structures semblables de surveillance électronique, s'inscrit dans ces problèmes de détermination de territoires. Echelon soulève cette difficulté supplémentaire qu'il met en lice plusieurs Etats, certains Parties à la Convention, d'autres pas. Autrement dit, l'extranéité inhérente à ce programme de surveillance transfrontalière pose divers problèmes en rapport avec la définition de ce fameux « territoire des droits de l'homme ».

Un de ces problèmes est l'imputabilité du fait internationalement illicite commis dans le cadre de la collaboration entre plusieurs Etats ou du fait de leurs organes à l'étranger en contrariété avec l'article 8 de la Convention; la question de l'imputabilité est analysée dans la deuxième partie du présent article. L'autre problème d'extranéité qui se pose en l'occurrence tient dans la question de savoir si un Etat peut respecter la Convention européenne des droits de l'homme en procédant à l'interception de communications par voie téléphonique ou électronique qui ne se passent pas sur son territoire, c'est-à-dire tous les cas dans lesquels les communications interceptées n'y entrent ou n'en sortent pas.

28. Droit international général et souveraineté territoriale —

Autrement formulée la question ici examinée est de savoir si un Etat peut ou non, sans violer le principe fondamental de la souveraineté territoriale et la Convention européenne des droits de l'homme, procéder à partir d'installations situées sur son territoire à l'interception de communications ne transitant à aucun moment par lui, ou même récolter sur son territoire le fruit d'écoutes internationalement illicites effectuées par un autre Etat participant à Echelon. Et ce quand bien même ces interceptions seraient conformes au droit de l'Etat qui y procède.

Le droit international général ne limite pas la compétence législative des Etats à leur seul territoire, plusieurs cas de figure pouvant se présenter (159).

(158) Cons. notamment le rapport 1998 du Conseil d'Etat français intitulé *Internet et les réseaux numériques*, lequel aborde en plusieurs endroits les problèmes de territorialité se posant pour le droit international privé, le droit pénal et le droit fiscal et prône dès lors la combinaison des mécanismes d'autorégulation du secteur et de la coopération internationale entre les Etats, en particulier par voie conventionnelle, en vue de ménager les souverainetés (« <http://www.internet.gouv.fr/francais/textesref/rapce98/sommaire.htm> »). Et aussi le mémoire de D.E.A. « Informatique et droit » présenté à l'Université de Montpellier I en 1998 par E. DE MARCO, *Le droit pénal applicable sur Internet*, disponible sur « <http://www.juriscom.net/universite/memoire6/penal.htm> ».

(159) Dans une littérature abondante, voyez notamment les diverses hypothèses développées par J. SALMON et E. DAVID, *Droit des gens*, t. II, 15^e éd., Presses Universitaires de Bruxelles, 1999-2000, pp. 240 à 246. Egalement D. TEZCAN, *Territorialité et conflits de juridictions en droit pénal international*, Ankara, Faculté des sciences politiques, 1983, pp. 56 et suiv.

L'hypothèse classique reste évidemment celle où la législation d'un Etat régit les faits et les personnes sur son territoire : c'est sa « compétence territoriale ».

Un Etat peut également régir par voie législative ses nationaux à l'étranger : c'est sa « compétence personnelle » (statut personnel en droit international privé tenant à l'octroi de la nationalité, statut militaire suivant les forces armées en déplacement, certains droits découlant de la citoyenneté, statut fiscal des résidents à l'étranger, certaines législations économiques,...). En matière pénale, l'Etat peut ainsi établir une législation qui s'applique parce que l'auteur d'une infraction est un des ses ressortissants (compétence personnelle active) ou parce que, au contraire, c'est la victime d'une infraction qui en est ressortissante (compétence personnelle passive).

Un Etat peut enfin promulguer une législation qui régit des étrangers à l'étranger : on en trouve certains exemples, parfois controversés, en matière économique. C'est toutefois en matière pénale que l'on rencontre le plus de telles législations qui n'étant ni territoriales, ni personnelles s'avèrent réellement extra-territoriales. On songe au principe de la « compétence universelle » qui permet la poursuite par n'importe quel Etat des crimes contre l'humanité commis dans un autre pays alors qu'aucun de leurs ressortissants n'en fut auteur ou victime. On songe surtout au principe de « protection » ou « compétence réelle » qui habilite un Etat à punir des actes commis en dehors de son territoire, même par des étrangers, par exemple en cas de falsification de sa monnaie, ou des actes qui constitueraient une atteinte à sa sécurité nationale.

A supposer même que les écoutes et interceptions organisées dans le cadre d'Echelon soient limitées à la prévention ou à la recherche d'infractions pénales ou qu'elles reposent sur des motifs de sécurité nationale (160), il n'en demeure pas moins que, si l'incrimination de certains comportements par une législation pénale au nom de la « compétence réelle » est une chose, l'accomplissement d'actes de contrainte se déployant à l'étranger en est une autre. Comme l'a posé très clairement la Cour permanente de Justice internationale,

*« la limitation primordiale qu'impose le droit international à l'Etat est celle d'ex-
clure, sauf l'existence d'une règle permissive contraire, tout exercice de sa puis-
sance sur le territoire d'un autre Etat. Dans ce sens, la juridiction est certaine-
ment territoriale; elle ne pourrait être exercée hors du territoire, sinon en vertu
d'une règle permissive découlant du droit international coutumier ou d'une
convention » (161).*

(160) Or il semble ressortir des informations disponibles que le programme Echelon permet de procéder aussi à de l'espionnage actif tant dans le domaine militaire qu'économique (cf. le démenti apporté par la chaîne de télévision NBC le 12 avril 2000 aux dénégations américaines).

(161) Cour permanente de justice internationale, arrêt du 7 septembre 1927, *affaire du Lotus*, Série A, n° 9, p. 18.

Et il ne fait aucun doute qu'une écoute téléphonique ou toute interception de message transmis par voie électronique emportent la contrainte dès lors qu'elles sont constitutives d'ingérences dans le droit au respect de la vie privée et de la correspondance, qu'elles aient lieu dans un cadre judiciaire, administratif ou militaire (162).

29. L'illicéité internationale des actes de contrainte à portée extra-territoriale — Pour les professeurs Dailler et Pellet, il résulte donc de la souveraineté territoriale que

« l'illicéité de tout acte de contrainte en territoire étranger est la conséquence nécessaire de l'interdiction de tout empiètement non autorisé par le souverain territorial »,

et que

« le droit international reconnaît aux Etats une compétence normative extra-territoriale; il exclut en revanche toute compétence d'exécution extra-territoriale forcée » (163).

C'est d'ailleurs en raison de ce principe fondateur du droit des gens qu'un jugement ou un acte administratif étrangers requièrent en principe un *exequatur* de la part des autorités, la plupart du temps judiciaires, de l'Etat tiers sur le territoire duquel l'acte juridique en question, qui suppose la contrainte, doit déployer ses effets.

Les principes inhérents à la souveraineté territoriale s'opposent ainsi à ce qu'un Etat A, même s'il peut conférer un champ d'application extra-territorial à sa législation, ne confère à ses actes de contrainte une portée extra-territoriale qui déploie ses effets sur le territoire d'un autre Etat B. Ceci peut également expliquer pourquoi certains requérants à titre individuel ne seraient pas tenus d'épuiser les voies de recours internes offertes, si elles existent, par le droit de l'Etat A (164). Ces principes entrent en jeu en ce qui concerne les écoutes téléphoniques puisque, comme l'enseignent les professeurs David et Salmon,

« il est a fortiori interdit à un Etat de procéder sur un territoire étranger, sans l'accord du souverain territorial, à des actes d'arrestation, d'instruction, d'enquête, de perquisition, à des enlèvements ou à des séquestrations » (165).

L'ensemble des éminents juristes issus du monde académique ou membres de juridictions internationales œuvrant aux travaux de l'Institut

(162) Voyez *supra* les n° 20 et suivants. Sur ce que « l'ingérence est d'abord une contrainte exercée sur une volonté », cons. V. COUSSIRAT-COUSTÈRE, « Article 8 § 2 », in L.E. PETTITI, E. DECAUX et P.H. IMBERT, *La Convention européenne des droits de l'homme — Commentaire article par article*, 2° éd., Paris, Economica, 1999, pp. 330-331.

(163) N. QUOC DINH (I), P. DAILLER et A. PELLET, *Droit international public*, 6° éd., Paris, L.G.D.J., 1999, respectivement p. 476 et p. 502.

(164) Voyez *infra* l'examen de l'article 13 de la Convention ainsi que des exceptions au principe de l'épuisement des voies de recours internes.

(165) J. SALMON et E. DAVID, *op. cit.*, p. 248.

de Droit International relatifs à la compétence extra-territoriale des Etats ont souscrit à ce point de vue (166). Le projet de résolution sur « *Les limites fixées par le droit international à la compétence des Etats sur les personnes relevant de leur juridiction* », présenté en janvier 1999 et devant encore être définitivement adopté, prévoit que l'Etat ayant le monopole des actes de coercition sur son territoire est par conséquent seul habilité à autoriser sur son territoire l'exercice d'actes de même nature par les organes d'un autre Etat; et ce avant l'accomplissement de tels actes (167). C'est le professeur Salmon qui a le mieux cerné au cours des débats de l'Institut la portée du respect du à la souveraineté territoriale lors d'enquêtes menées à l'étranger :

« Pour les enquêtes exercées par ses propres organes afin de recueillir des témoignages, même sans coercition, ni intimidation, je suis plus réticent. A fortiori s'il y a coercition ou intimidation. J'estime que de telles mesures doivent faire l'objet d'une demande d'autorisation, quitte à ce que l'Institut propose que l'Etat sur le territoire duquel s'effectuera l'enquête donne son accord lorsqu'il a l'assurance que les droits des personnes, y compris le respect de la vie privée, sont adéquatement protégés et à condition que, par son objet ou ses méthodes, l'enquête ne soit pas contraire au droit de l'Etat du for » (168).

L'Etat du for doit donc donner son consentement préalable à l'acte de coercition ou d'exécution forcée. Le point I.3. du projet de résolution de l'Institut a opté pour une conception large de la notion de contrainte. La contrainte n'est pas limitée à la contrainte physique, les formes indirectes

(166) *Ann. IDI*, vol. 68-I, 1999, sur les travaux préparatoires de la session de Berlin en 1998. Consultez en particulier les divers rapports de F. RIGAUX (p. 440, p. 480, pp. 507-561) et les diverses prises de position de M. BEDJAOUI (pp 446-447 et spéc. pp. 568-570 dans lesquelles le juge à la CIJ souligne la nature particulière de l'article 1^{er} de la CEDH quant aux obligations des Etats et aux droits des individus confrontés à des actes extra-territoriaux), F. MATSCHER, juge à la Cour européenne des droits de l'homme (p. 457), A. VON MEHREN (p. 463), J. SALMON (pp. 469-470), et K. ZEMANEK (p. 475). Ces juristes ont également insisté à plusieurs reprises sur ce que l'acte de coercition ne se résument pas à l'emploi de la contrainte physique.

(167) Le texte du projet de résolution est reproduit in. *Ann. IDI*, 1999, pp. 602-605. Voyez en particulier le point II. : « 1. Les règles de droit international qui tendent à délimiter les compétences territoriales des Etats sur les personnes relevant de leur juridiction risquent d'être inopérantes si ces personnes ne peuvent se prévaloir dans l'ordre interne de la transgression de l'une de ces règles par l'organe de l'Etat qui était tenu de les prendre en considération.

2. De telles règles de droit international devraient dès lors être interprétées en ce sens que leur violation puisse être invoquée par la personne ou l'entreprise aux droits de laquelle elle a infligé un dommage. Pareils effets de la règle de droit international dans l'ordre interne ne devraient pas être influencés par l'attitude qui aurait été prise par l'Etat à la compétence duquel la transgression de la même règle aurait porté atteinte après que celle-ci a eu lieu.

3. Quand la violation du droit international a en outre eu pour effet de porter atteinte à un droit fondamental garanti à la personne par un traité international ou par la Constitution de l'Etat sur le territoire duquel pareille violation a été commise ou à la compétence duquel elle peut être rattachée, le titulaire de ce droit fondamental doit être en mesure de le faire prévaloir sur l'exercice de la compétence étatique ».

(168) Ces propos de J. SALMON figurent aux pages 469 et 470 de l'*Ann. IDI*, 1999.

comme la menace de contrainte étant également visées (169). Même si les interceptions téléphoniques modernes ne se font plus guère par raccordement d'une prise de casque sur les commutateurs ou par pose d'un compteur dénombrant les conversations entrantes et sortantes, la contrainte est bel et bien présente de par l'ingérence dans la vie privée que représente toute forme de captation, y compris des émissions de messages par voie de satellite. Les principes juridiques en cause demeurent intégralement les mêmes.

Au regard de l'article 8 de la Convention européenne des droits de l'homme en particulier, il ne faut pas oublier que l'opération juridique de contrôle de la conformité de l'interception téléphonique s'effectue en deux temps. Vient d'abord l'examen de l'existence d'un acte juridique, d'un fait ou d'une omission de l'autorité qui constituent autant d'ingérences possibles (donc de potentiels actes de contrainte) dans le droit au respect de la vie privée (article 8, § 1^{er}). Ce n'est qu'ensuite seulement qu'il est procédé à l'examen successif de la présence des trois conditions cumulatives de légalité, de légitimité et de nécessité, dont la réunion seule permet, le cas échéant, d'estimer l'interception comme valable (article 8, § 2). C'est vrai en ce qui concerne les écoutes sauvages relevant de l'espionnage comme en ce qui concerne les tentatives de régler unilatéralement les questions soulevées par les difficultés indéniables que pose notamment la criminalité informatique pour le principe de territorialité.

30. La souveraineté territoriale est au cœur des débats d'actualité sur la recherche et la répression de la cyber-criminalité — La section du rapport et des études du Conseil d'Etat français était très clairement consciente des problèmes suscités par les spécificités d'Internet quand elle a remis son rapport 1998. Mais elle a manifestement préféré voir dans le principe de territorialité, même sans trop d'illusions, une possibilité d'éviter la création de « paradis virtuels » et de soumettre les réseaux informatique au droit plutôt qu'un obstacle dirimant pour l'émergence d'une régulation des autoroutes de l'information (170).

Seule la coopération internationale peut non seulement arriver à circonscrire les nouvelles formes de délinquance mais aussi atteindre cet objectif dans un cadre respectueux des souverainetés, sans quoi l'unilatéralisme

(169) « La notion de contrainte ne saurait être limitée aux actes matériels de coercition physique exercées sur une personne ou sur un bien. Le critère de localisation qui s'applique correctement à de tels actes est impuissant à saisir d'autres formes de contrainte, telles que la menace du recours à la force, de la privation d'un bien ou de sanctions économiques. Le seul énoncé de telles menaces qui ne sauraient être mises à exécution que sur le territoire de l'Etat des autorités duquel elles émanent est de nature à exercer une forme de contrainte sur le comportement de leurs destinataires en quelque lieu que ce soit, contrainte qui pour être indirecte n'en est pas moins certaine ».

(170) Voyez en particulier dans le rapport précité sur Internet et les réseaux numériques, le point 3. (« Faciliter l'action de la police et de la justice ») de la 4^e partie (« Lutter contre les contenus et comportements illicites »), « <http://www.internet.gouv.fr/francais/textesref/rapce98/rap4.htm> », page 23 sur 59 ainsi que les suivantes.

reprendrait le dessus (unilatéralisme qui est précisément l'un des reproches majeurs qui peut être adressé à Echelon puisqu'un petit nombre d'Etats agissant plus ou moins de concert peuvent capter des messages publics ou privés échangés dans l'immense majorité des autres Etats).

La Recommandation n° R (95) 13 du Comité des Ministres du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information se prononçait ainsi sans ambiguïté contre les perquisitions extra-territoriales unilatérales dans les réseaux informatiques :

« Le pouvoir d'étendre la perquisition à d'autres systèmes informatiques devrait être également applicable lorsque le système se trouve sous une juridiction étrangère, à condition qu'une action immédiate soit requise. En vue d'éviter d'éventuelles violations de la souveraineté des Etats ou du droit international, une base légale explicite devrait être créée pour de telles perquisitions ou saisies étendues. Par conséquent, il y a besoin urgent de négocier des instruments internationaux quant à la question de savoir comment, quand et dans quelle mesure de telles perquisitions ou saisies peuvent être permises » (171).

Les récentes attaques de pirates informatiques contre certains sites Internet ont poussé le Conseil de l'Europe à dévoiler, le 27 avril 2000, l'état des négociations en cours entre les Etats membres ainsi qu'avec l'Afrique du Sud, le Canada, les Etats-Unis et le Japon à propos du projet de Convention sur la cyber-criminalité.

L'une des pierres d'achoppement reste la manière d'organiser les perquisitions et saisies des données informatiques stockées au regard du principe de territorialité (article 14); il en va de même en ce qui concerne les interceptions téléphoniques (article 18 réservé au moment de la rédaction de ces lignes). La détermination de la compétence législative pour incriminer les comportements punissables demeure très classique dans le projet puisqu'elle est appelée à être territoriale, et par extension classiquement fondée sur la loi du pavillon ou de l'immatriculation en ce qui concerne les navires, aéronefs et satellites, d'une part, et personnelle si l'infraction par un ressortissant est punissable là où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun Etat, d'autre part (article 19.1). Pour le reste, c'est la coopération internationale qui doit présider aux investigations, aux procédures et à la récolte des preuves électroniques (articles 20 et suivants) (172).

31. La tentation de l'unilatéralisme en procédant à des perquisitions, saisies et copies informatiques extra-frontalières : le cas belge — Compte tenu de ces débats intergouvernementaux qui pour être houleux n'en trouveront pas moins bientôt une solution, c'est à raison que

(171) Point 17 de l'annexe à la Recommandation n° R (95) 13, adoptée le 11 septembre 1995, « <http://www.coe.fr/cm/ta/rec/1995/f95r13.htm> ».

(172) Pour le communiqué de presse du Conseil de l'Europe, le texte du projet de Convention et les notes explicatives sur l'état des négociations : « <http://conventions.coe.int/treaty/FR/projets/cybercrime.htm> ».

la section de législation du Conseil d'Etat belge a rendu un avis qui critique fort sévèrement le projet de loi sur la criminalité informatique en cours d'examen au Parlement (173). En cause notamment, la volonté d'insérer un nouvel article 88^{ter} dans le Code d'instruction criminelle la possibilité pour le juge d'instruction de procéder à la saisie de données informatiques qui ne peuvent être que copiées si elles ne se trouvent pas sur le territoire belge. Dans ce cas, le juge d'instruction, par l'intermédiaire du parquet, devrait en informer le Ministre de la Justice qui en informerait à son tour les autorités compétentes de l'Etat concerné.

C'est donc un système d'information *a posteriori* qui est projeté. Contrairement à ce qu'affirme le Ministre de la Justice dans l'exposé des motifs du projet de loi, le rappel des principes du droit des gens opéré par la Recommandation n° R (95) 13 est correct. La justification selon laquelle cette procédure d'information n'entraînerait pas de violation intentionnelle de la souveraineté d'un autre Etat (174) est irrelevante puisque, comme le pose justement le point I.1. du projet de résolution précité de l'Institut de Droit International, l'accord du souverain territorial doit être exprimé avant l'accomplissement de l'acte de coercition (175).

Est également erronée la justification tirée de l'extension par analogie du mécanisme de « *hot pursuit* » existant en droit maritime international (176). D'abord parce que ce mécanisme est une exception au principe de la souveraineté territoriale, ensuite parce que la « *hot pursuit* » est strictement réglementée par la coutume internationale codifiée dans l'article 111 de la Convention de Montego Bay sur le droit de la mer (177).

Malgré les débats intervenus devant la Commission de la Justice de la Chambre, le projet de loi sur la criminalité informatique, en ce qu'il permet les saisies informatiques transfrontalières, n'a donc pas suivi l'avis du

(173) Le Sénat a retourné à la Chambre le 13 juillet 2000 le projet amendé mais qui n'avait pas été modifié en ce qui concerne le point ici discuté.

(174) Exposé des motifs du double projet de loi sur la criminalité informatique, *Doc. parl., Chambre*, s.o. 1999-2000, 50 0213/001 et 50 0214/001, p. 11. L'exposé affirme plus loin que la procédure classique de la commission rogatoire ne sera suivie que si le temps et les connaissances le permettent (p 24).

(175) Le point I.1. du projet de résolution, évoqué plus haut, dispose que « *l'Etat exerce sur l'étendue de son territoire le pouvoir exclusif d'accomplir des actes matériels de coercition sur les personnes et d'exécution forcée sur les biens et celui d'autoriser, avant leur accomplissement, l'exercice d'actes de même nature par les organes d'un autre Etat* ». C'est nous qui soulignons.

(176) L'argument a été exprimé dans l'exposé des motifs du projet de loi (p 25) et fort discuté devant la Commission de la Justice de la Chambre, certains membres s'y montrant hostiles et d'autres favorables : rapport de M. VERHERSTRAETEN du 24 mars 2000, *Doc. parl., Chambre*, s.o. 1999-2000, 50 213/004, pp. 19, 20, 21, 25, 61 et suiv. Le projet de nouvel article 88^{ter}, § 3, du Code d'instruction criminelle n'a cependant pas été adapté dans le sens de sa mise en conformité avec le droit international public.

(177) Sur les nombreuses conditions cumulatives de mise en œuvre du droit de poursuite, voyez l'arrêt au fond du Tribunal International du Droit de la Mer rendu le 1^{er} juillet 1999 dans l'*Affaire du navire Saiga* (n° 2), §§ 145 et suivants : « <http://www.un.org/Depts/los/ITLOS/Judg-F.htm> ». A ce sujet : Ch. DE VISSCHER, *Problèmes de confins en droit international public*, Paris, Pedone, 1969, pp. 173 et suiv.

31 mai 1999 du Conseil d'Etat. Celui-ci rapportait pourtant avec exactitude les règles applicables en l'absence de convention internationale sur les flux informatiques :

« parmi les règles fondamentales du droit international figure celle selon laquelle l'Etat exerce l'autorité étatique sur son propre territoire, et le fait seul, à l'exclusion de tout autre Etat. Il en découle qu'en temps de paix, il est absolument interdit à un Etat de procéder à une fonction de contrainte sur le territoire d'un autre Etat. Ceci concerne notamment tous les actes de la fonction exécutive, liés ou non à la justice. Un Etat ne peut ainsi en dehors de son territoire, ni procéder à une arrestation, ni dresser un procès-verbal constatant un délit, ni mener une enquête, etc. La jurisprudence internationale est, sur ce point, constante ».

Le Conseil d'Etat ajouta que

« la Belgique ne peut pas non plus par une loi propre établir un mode particulier de coopération entre ses autorités judiciaires ou policières et celles des autres Etats. Ces modalités de coopération entre la Belgique et de nombreux autres pays européens ont, en effet, été arrêtées par des traités qui constituent autant d'exceptions au principe de la territorialité exclusive. Ces traités attestent donc à la fois l'existence de ce principe et le fait que les Etats tiennent à ce qu'il soit respecté, sauf dans les cas exceptionnels que ces traités prévoient et selon les modalités qu'ils précisent » (178).

Ces affirmations sont d'autant plus importantes que si l'administration de la preuve est libre en droit pénal, le juge ne peut établir sa conviction que sur base des éléments régulièrement obtenus, notamment au regard de l'article 8 de la Convention européenne des droits de l'homme, et soumis à libre contradiction (179).

La tentation de l'unilatéralisme est donc là mais sa présence ne permet en rien de déroger aux fondamentaux du droit des gens (180). Avec la circonstance aggravante, en ce qui concerne le programme Echelon, que l'on ne se situe pas dans un cadre qui sera tôt ou tard soumis aux impératifs de la coopération judiciaire internationale mais que l'on est bel et bien confronté à un système de surveillance administrative de type unilatéral dans la mesure où seuls les Etats participants bénéficient du fruit de ce système d'espionnage.

32. Une illicéité des écoutes téléphoniques extra-frontalières confirmée explicitement en l'état actuel du droit communautaire —

Pour achever de se convaincre, on doit relever que, en ce qui concerne au moins les Etats membres de l'Union Européenne (tous parties à la Conven-

(178) Avis du Conseil d'Etat sur l'avant-projet de loi relatif à la criminalité informatique, *Doc. parl.*, Chambre, s.o. 1999-2000, 50 0213/001 et 50 0214/001, respectivement pp. 45 et 47.

(179) Avis sur l'avant-projet de loi relatif à la criminalité informatique, *ibidem*, p. 48.

(180) On notera d'ailleurs que, même en ce qui concerne l'organisation conjointe de l'Euro 2000 de football où il paraît évident que la Belgique et les Pays-Bas devaient coopérer en vue du maintien de l'ordre, l'intervention policière transfrontalière a fait l'objet d'un traité détaillé signé par les deux pays le 26 avril 1999 à Bergen-op-Zoom (la loi d'assentiment du 28 avril 2000 est publiée au *Moniteur belge* 26.05.2000).

tion européenne des droits de l'homme, faut-il le rappeler), les règles nouvelles qui gouvernent la coopération judiciaire et policière (les politiques dites du « troisième pilier ») ont abordé la question de l'extranéité des écoutes téléphoniques.

En effet, le problème de l'application extra-territoriale de ces actes de contrainte a été soulevé dans la Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications. La Résolution vise à élaborer un catalogue des spécifications techniques requises des opérateurs de réseaux et fournisseurs de services dans le cadre des interceptions (181). Ce texte résulte des pressions américaines sur l'Union pour qu'elle pousse également l'industrie des télécommunications à faciliter les interceptions de communications (182). Mais la première phrase du préambule est sans ambiguïté aucune, les Etats de l'Union Européenne

« réaffirmant la nécessité de respecter, dans la mise en œuvre des mesures d'interception des télécommunications, le droit des personnes physiques au respect de la vie privée consacré par les législations nationales territorialement applicables » (183).

Consulté sur un autre projet de résolution du Conseil ayant le même objet, le Parlement européen a relevé également que

« la résolution n'est pas contraignante et n'habilite en aucun cas les services de la sûreté à procéder à des interceptions en dehors de la zone relevant de la juridiction nationale. En outre, elle ne modifie en rien les dispositions régissant l'interception légale des télécommunications dans les différents Etats membres. Aussi n'affecte-t-elle pas l'équilibre délicat existant entre le respect des droits fondamentaux et la sécurité intérieure » (184).

Les autorités de l'Union européenne et des Etats qui la composent sont bel et bien pleinement conscientes de ce qu'un acte de contrainte purement extra-territorial, pour ne pas parler des écoutes « sauvages » manifestement en-dehors du champ des résolutions à l'étude, conduirait à de graves problèmes, en particulier pour les droits fondamentaux (185). L'Allemagne et le Royaume Uni, quel que soit leur rôle dans le programme Echelon, sont

(181) Le rapport « Elliott » (p 6) souligne que la Résolution du Conseil de 1995 vise toutes les formes possibles de télécommunications. Le rapport technique précité de mars 2000 de l'E.T.S.I. sur les interceptions légales de télécommunications est donc aussi en partie la résultante de ces pressions américaines.

(182) Rapport « Becker », pp. 19-20; rapport « Elliott », p. 6.

(183) J.O.C.E. n° C 329 du 04/11/1996, pp. 1-6; c'est nous qui soulignons (près de deux ans se sont écoulés entre l'adoption et la publication!).

(184) Commission des libertés publiques et des affaires intérieures, rapport du 23 avril 1999 de Mr G. SCHMID sur le projet de résolution du Conseil relative à l'interception légale des télécommunications compte tenu des nouvelles technologies, PE 229.986/déf., p. 7. Voyez *supra* les reproches adressés aux autorités européennes dans le domaine des interceptions électroniques.

(185) Nous parlons ici d'écoutes purement extra-territoriales dans la mesure où les résolutions en cause ne s'opposent pas *a priori* à l'interception des communications entrant ou sortant du territoire de l'Etat qui y procède.

membres de l'Union européenne et ne peuvent donc ignorer le contenu de ces résolutions du Conseil des Ministres (186).

Sans se pencher explicitement sur le cas des écoutes extra-territoriales, l'article 5 de 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 enjoint aux Etats de garantir la confidentialité des communications sur les réseaux publics ou accessibles au public et prohibe toute forme d'espionnage commercial (187).

33. La question de l'éventuelle extra-territorialité d'une interception ne peut être réglée que de l'accord des Etats sur le territoire desquels elles ont lieu comme en attestent les débats en cours au Parlement européen — La question de l'extra-territorialité des interceptions électroniques est à ce point brûlante que par Résolution législative du 17 février 2000 le Parlement européen a sévèrement enjoint au Conseil de revoir en profondeur son projet d'acte établissant une convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union (188).

Sans remettre en cause l'utilité des écoutes demandées par un Etat requérant à un Etat requis dans le cadre de l'entraide judiciaire, le projet d'article 16, § 1^{er}, revu par le Parlement prévoit ainsi que la demande d'entraide doit être préalable, ce qui se passe de commentaires dans le cadre d'Echelon. De même, le projet d'article 16, § 3, stipule, parmi d'autres conditions détaillées, qu'il convient de confirmer qu'un ordre ou mandat d'interception régulier a été émis dans le cadre d'une enquête pénale, ce qui interdirait l'usage de l'entraide à des fins d'écoutes militaires ou administratives; le § 9bis impose d'ailleurs que l'écoute soit toujours décidée par un juge. La durée des interceptions de télécommunications doit être communiquée préalablement à l'Etat requis. Et selon le § 5 de cet article 16 adopté par le Parlement, l'Etat requis doit pouvoir toujours subordonner son

(186) Le rapport « Becker » au Parlement européen (p 22) rappelle en outre que, en l'absence de texte communautaire contraignant qui régleme les interceptions légales de communications, les Etats membres, comme ils sont tous signataires de la C.E.D.H., doivent veiller à respecter celle-ci telle qu'elle est appliquée par la Cour européenne des droits de l'homme.

(187) La Directive 97/66/CE s'applique dans les domaines couverts par le droit communautaire, c'est-à-dire essentiellement en matière de relations économiques, les domaines tels la sécurité nationale restant de la compétence des Etats. Son article 5 porte que « les Etats membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessibles au public. En particulier, ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées, conformément à l'article 14, § 1 ». Cette disposition interdit dès lors toute forme d'espionnage électronique économique.

(188) La Résolution législative a été adoptée en séance plénière du 17 février 2000, A5-0019/2000.

accord au respect des conditions qu'il imposerait si la demande émanait de ses propres services.

La meilleure preuve du caractère pour le moins délicat de l'éventuelle extra-territorialité des interceptions réside cependant dans la suppression par le Parlement de l'article 18 du projet de convention sur l'entraide pénale rédigé par le Conseil. Il aurait permis l'interception de cibles sur le territoire d'un Etat sans son assistance technique. Cette suppression est ainsi justifiée :

« Il est proposé de supprimer cet article étant donné qu'il est très controversé : d'une part, il pourrait limiter les activités de renseignement destinées à assurer l'intégrité d'un Etat membre et, d'autre part, il pourrait donner la possibilité à des organes d'enquête d'un Etat membre d'effectuer des interceptions dans un autre Etat membre, sans l'aval ou l'autorisation de ce dernier. Il serait en principe judicieux de mener une réflexion plus approfondie sur ce thème, avant de le codifier dans une convention de l'Union » (189).

La question de l'extra-territorialité des écoutes téléphoniques et des mécanismes y apparentés doit donc être débattue avant d'être éventuellement tranchée, sa résolution ne pouvant en outre n'intervenir que par voie conventionnelle dans la mesure où les Etats concernés aliéneraient une parcelle de souveraineté (190).

A supposer qu'existent bien, sur le plan matériel, des législations nationales (ou des accords internationaux qui peuvent en tenir lieu dans le cadre de la Convention européenne des droits de l'homme) qui autorisent les Etats qui participent au programme Echelon à procéder des écoutes, il n'en demeure pas moins qu'elles ne peuvent passer comme étant des « lois » au sens de l'article 8, puisque les actes de contrainte que sont les écoutes ont

(189) Rapport de Mr A. DI PIETRO, au nom de la Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures, sur le projet d'acte du Conseil établissant la convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, 31 janvier 2000, PE 232.057/déf., p. 38. Adde les pages 50 et 51.

(190) Comme le concluait K.-G. PARK, *La protection de la souveraineté aérienne*, Paris, Pedone, 1991, malgré les progrès de la conquête spatiale, la souveraineté aérienne reste aussi le meilleur moyen de protection de l'immense majorité des Etats, qui n'y ont pas accès ni aux nouveaux modes d'armement. Si la délimitation exacte entre espace aérien atmosphérique et extra-atmosphérique n'est toujours pas arrêtée, la souveraineté étatique pleine et entière est reconnue dans le premier cas par l'article 1^{er} de la Convention de Chicago de 1944. Quant à l'espace extra-atmosphérique, le Traité de 1967 sur son exploration et son utilisation le soustrait certes à toute souveraineté étatique (adde J. VERHOEVEN, *Droit international public*, Bruxelles, Larcier, 2000, pp. 581-597). Néanmoins, dans les cas d'interceptions à l'aide de satellites ou d'autres stations terrestres de communications électroniques transmises par voie de satellite, il faut bien tenir compte de ce que la base où aboutit un message intercepté est bien située sur le territoire d'un Etat B après être parti du territoire d'un Etat A. L'éventuelle phase pendant laquelle un message échapperait, dans le seul espace extra-atmosphérique, à toute souveraineté étatique, et en admettant qu'une utilisation pacifique dudit espace autorise l'interception du message, est de toute façon de l'ordre de quelques secondes tout au plus; il quitte forcément un territoire pour être « rapatrié » vers un autre. Autrement dit, en ce qui concerne Echelon, une conversation téléphonique de Belgique vers le Portugal qui serait captée à la base de Menwith Hill doit rester protégée par le droit des Etats de départ et d'arrivée et ne peut donc, juridiquement, être captée par la NSA et le GCHQ à l'insu total des personnes qui la mènent.

un effet extra-territorial qui les place en contradiction manifeste avec les principes les plus élémentaires du droit international. Et quand bien même de telles « lois » existeraient, leur absence de publicité les rend difficilement opposables aux ressortissants et résidents étrangers des Etats parties à Echelon (191). Sans compter qu'elles ne sauraient de toutes façon pas être opposées aux ressortissants et résidents étrangers sur le territoire d'Etats tiers à ceux participant à Echelon (192). A plus forte raison encore si le droit des ces Etats tiers protège la vie privée dans une mesure supérieure à la Convention européenne des droits de l'homme, notamment lorsqu'ils prohibent certaines formes d'écoutes téléphoniques sur leur territoire.

Ces mêmes principes sous-tendent également la règle du « Safe Harbour » qui fait l'objet d'âpres querelles entre les Etats Unis qui y sont opposés et les pays européens. Cette règle postule qu'un transfert international de données à caractère personnel, par voie informatique ou autre, ne peut être autorisé que si l'Etat de destination offre un niveau de protection « *adéquat* » du droit au respect de la vie privée (193).

En raison des principes inhérents au respect de la souveraineté territoriale qui viennent d'être rappelés, la Résolution sur le système Echelon adoptée le 11 avril 2000 par la Commission des Libertés du Parlement européen ne se trompe pas en affirmant que

« (...) en principe, toute forme d'interception par un Etat membre (doit être) notifiée aux autres Etats membres où se trouvent les personnes interceptées » (194).

(191) *Infra* quant au défaut d'« accessibilité » des normes censées régir Echelon.

(192) Qui plus est, le nouveau *Regulation of Investigatory Powers Act 2000* britannique stipule bien en sa clause 2.(4) que ne sont autorisées que les interceptions de communications entrant ou sortant du Royaume Uni. Les interceptions en-dehors de ce cadre ne seraient de toute façon pas conformes au droit britannique lui-même et violeraient donc bien la condition de légalité exigée par l'article 8 pour défaut de respect du droit interne.

(193) C'est afin de supprimer toute ambiguïté à ce propos que, sur demande de l'Assemblée parlementaire du Conseil de l'Europe, le comité consultatif de la Convention n° 108 de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a rendu public le projet de protocole additionnel à celle-ci, dont l'article 2, § 1^{er}, dispose que « *chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré* ». Les dérogations à ce principe ne sont possibles que si le droit interne le prévoit ou si le responsable du transfert présente des garanties contractuelles suffisantes. Mais dans tous les cas, il est certain que la décision de transfert doit émaner d'un organisme indépendant dont la décision doit être soumise à un contrôle juridictionnel (article 1^{er} du projet de protocole), d'une part, la décision de transfert ne pouvant être prise qu'après vérification « au cas par cas » du niveau de protection offert par l'Etat de destination. Voyez le point 27 du rapport explicatif du projet de protocole additionnel à la Convention n° 108 du Conseil de l'Europe, 8 juin 2000, « http://www.coe.fr/dataprotection/Treaties/projet_20de_20protocole_20F.htm ».

(194) Point L des considérants préliminaires de la résolution « *Watson* » précitée. Le point G estime de manière générale que les interceptions menées dans le cadre de la lutte contre le crime « transfrontières » doivent être réglées par la future convention sur la cyber-criminalité négociée au sein du Conseil de l'Europe et avec la plupart des grands pays industrialisés, laquelle réserve en l'état des travaux le cas des interceptions et saisies transfrontalières.

c. *Echelon contre le principe de l'application de la clause la plus favorable à la protection des droits portés par la Convention*

34. L'exemple de la prévalence que le droit belge doit avoir, sur le territoire belge, sur toute autre norme : de la prohibition absolue des écoutes... — Au titre du contrôle de « légalité » toujours, il ne faut pas non plus perdre de vue l'article 53 (anciennement 60) de la Convention qui fait prévaloir sur elle une autre règle, nationale ou internationale, si cette règle est plus favorable à la protection d'un droit garanti par ailleurs par la Convention (195). Si l'on prend, par exemple, en considération parmi les droits nationaux des pays signataires de la Convention le cas du droit belge, il faut bien savoir que pendant des années l'article 17 de la loi du 13 octobre 1930 coordonnant les différentes dispositions législatives concernant la télégraphie et la téléphonie interdisait de manière absolue les écoutes téléphoniques, qu'elles soient publiques ou privées, judiciaires ou administratives (196).

Si la Cour de cassation a pu estimer valides les écoutes judiciaires régulièrement effectuées sous l'empire d'un droit étranger à l'époque de la prohibition absolue, et à la condition que l'article 8 de la Convention ait été respecté, on pouvait estimer que cela constituait un pis-aller vu l'absence de réglementation en droit belge (197). C'était certes déjà très contestable au regard de la prohibition absolue, d'une part, et de la Convention, d'autre part (198). La prohibition absolue des écoutes a de toute façon abouti au constat de la contrariété avec l'article 8 des procédés de comptage des conversations (199).

(195) J. DE MEYER, « Brèves réflexions à propos de l'article 60 de la Convention européenne des droits de l'homme », in. *Mélanges G.J. Wiarda*, Cologne, Karl Heymanns Verlag, 1988, pp. 125-129; E. DECAUX, « Article 60 », in. L.E. PETITTI, E. DECAUX et P.H. IMBERT (dir.), *La Convention européenne des droits de l'homme — Commentaire article par article*, 2^e éd., Paris, Economica, 1999, pp. 897-903 qui affirme que cet aspect de l'article (53), la plupart du temps invoqué pour affirmer au contraire la primauté de la Convention, n'a guère de portée pratique. Cela semble, dans le cas particulier qui nous occupe, pour une fois devoir être démenti.

(196) Liège (ch. mis. acc.) 22 septembre 1988, *J.T.* 1988, p. 655 qui a invalidé des écoutes effectuées par une entreprise à l'encontre de certains de ses préposés. Voyez également les critiques parfaitement justifiées de F. RIGAUX sur Bruxelles 15 mars 1994, *J.T.* 1994, p. 658.

(197) Cass. 24 mai 1983, *Pas.* 1983, I, p. 511; Cass. 19 février 1985, *Pas.*, I, p. 370; Cass. 10 avril 1990, *Pas.* 1990, I, p. 1052; Cass. 26 janvier 1993, *Pas.* 1993, I, p. 101. Cass. 30 mai 1995, *Pas.* 1995, I, p. 558, a appliqué le même principe en ayant également égard à l'article 17 du Pacte international relatif aux droits civils et politiques. La loi étrangère doit également avoir été respectée (Cass. 25 avril 1996, *Pas.* 1996, I, p. 133). Tous ces cas concernaient des écoutes effectuées aux Pays-Bas.

(198) La preuve en droit pénal a beau être libre en principe, on ne peut écarter le principe de loyauté qui doit présider à son établissement. Voyez les interrogations critiques sur cette jurisprudence qu'a formulées D. GARABEDIAN dans son commentaire sous Bruxelles, 30 novembre 1984, *J.T.* 1985, p. 736.

(199) Cass. 2 mai 1990, *J.T.* 1990, p. 469, note J.M. qui indique que la Cour a ainsi tranché la controverse sur la (non-)compatibilité du comptage avec la Convention. Et les observations de J. MILQUET, « Quand sonne le glas du Zoller? », *Journ.Proc.*, n° 178, 21 septembre 1990, p. 34.

La prohibition des écoutes téléphoniques n'est plus absolue en droit belge. Du moins celles-ci sont-elles sévèrement encadrées et seulement autorisées dans les cas prévus par la loi.

35. ... à leur stricte réglementation qui persiste à prohiber toutes les écoutes administratives effectuées sur le territoire belge — La loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées a introduit certaines prohibitions très strictes dans le Code pénal. Le principe contenu dans le nouvel article 259bis du Code pénal est la prohibition des écoutes opérées par les fonctionnaires qui s'exposent à des peines très lourdes. Il ne peut être dérogé au principe que si l'écoute intervient dans les cas et en respectant les formalités prévues par la loi, hypothèse qui, en l'état du droit belge, n'est rencontrée que dans les cas prévus par le Code de procédure pénale. L'article 259bis du Code pénal comporte par ailleurs un § 4 qui résulte de l'article 44 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. Cette disposition stipule que l'article 259bis, § 1^{er}, 1^o (écoute, connaissance, enregistrement de communications privées sans l'accord de tous les participants à celles-ci) ainsi que le § 1^{er}, 2^o (fait de procéder à une installation quelconque avec l'intention de commettre l'une de ces infractions) ne s'appliquent pas à la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service général du renseignement et de la sécurité des forces armées, à des fins militaires, de radiocommunications militaires émises à l'étranger (200). C'est le seul cas éventuel, car sa rédaction cadre mal avec l'exigence de prévisibilité, où les écoutes purement administratives sont autorisées. On peut donc déjà en conclure que la captation administrative des communications privées est, en principe, formellement interdite (201); faute d'indication contraire, l'interdiction est valable tant sur le territoire belge que pour les écoutes procédées à l'étranger.

La loi du 30 juin 1994 a aussi inséré un nouvel article 314bis dans le Code pénal en étendant l'interdiction des écoutes à « *quiconque* », c'est-à-dire agent public ou personne privée, capte sous quelque forme que ce soit toute communication privée sans l'accord de tous ses participants. Sont également incriminées la divulgation du fruit d'écoutes illégales mais aussi l'uti-

(200) L'article 259bis, § 5, du Code pénal est très mal rédigé. En effet, il vise expressément les radiocommunications militaires alors que le § 1^{er} qu'il rend partiellement inapplicable aux écoutes du SGR vise tout aussi expressément les communications privées! A notre connaissance, le Roi n'a toujours pas fait entrer en vigueur cette disposition qui pose également problème au regard de l'interdiction des actes de contrainte extra-territoriaux.

(201) L'article 12 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité plaide également en ce sens puisque ceux-ci ne peuvent, pour accomplir leur mission, utiliser des moyens de contrainte que dans les conditions prévues par la loi. Les dispositions sur le recueil, la communication et la conservation des données ne parlent pas des écoutes comme moyen de les rassembler, ni de pouvoir remplir les missions de protection des personnes. La Sûreté de l'Etat, service intérieur, ne dispose d'aucune habilitation légale en la matière.

lisation frauduleuse ou à dessein de nuire d'écoutes légalement opérées. Les écoutes privées ou leur utilisation à des fins privées sont donc également prohibées par le Code pénal. Faute d'indication contraire, la prohibition des écoutes privées est également valable tant en Belgique qu'à l'étranger.

Le Code d'instruction criminelle ne permet ainsi les écoutes judiciaires que dans les conditions strictement circonscrites par ses articles 90^{ter} à 90^{decies}, également introduits par la loi du 30 juin 1994. Elles ne peuvent être ordonnées que par le juge d'instruction, à titre exceptionnel, et uniquement pour les infractions limitativement énumérées; le juge d'instruction ne peut commettre à ce type de mesures de surveillance que des officiers de police judiciaire; le Ministre de la Justice est obligé de faire annuellement rapport au Parlement (202).

Dès lors, sur le territoire belge, c'est le droit belge, s'il se trouve en conformité avec la Convention qui, doit prévaloir sur celle-ci puisqu'il est plus restrictif qu'elle en ce qui concerne le recours aux écoutes (203) et, par tant, plus protecteur du droit au respect de la vie privée (204). En effet, le droit belge continue à prohiber de manière absolue sur le territoire belge les écoutes administratives quelles qu'elles soient; aucun acte matériel, aucune disposition juridique en provenance d'Etats tiers ne peuvent donc y être appliqués. De telle sorte que toute écoute administrative effectuée en Belgique ou au détriment de personnes s'y trouvant doit être réputée comme n'étant pas prévue par la « loi ». L'état du droit belge s'impose tant aux

(202) Ces conditions sont très strictes : le mandat d'arrêt qui repose sur des écoutes ne les respectant pas doit être invalidé (Cass. 26 juin 1996, *Pas.*, 1996, I, p. 263).

(203) Voyez également l'article 109^{ter} D de la loi du 21 mars 1991 relative à la réforme de certaines entreprises publiques (introduit par la loi de libéralisation des télécommunications du 19 décembre 1997) qui sous réserve de l'accord des personnes concernées interdit aussi, notamment, à « quiconque », qu'il agisse personnellement ou par l'entremise de tiers de « prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunications en provenance d'autres personnes et destinées à celles-ci ». L'article 109^{ter} E, § 1^{er}, rend cette disposition ainsi que les articles 259^{bis} et 314^{bis} du Code pénal inapplicables dans trois cas :

— lorsque la loi (au sens formel d'acte législatif et non matériel de la Convention) permet ou impose l'accomplissement des actes visés (il n'en existe pas d'autres cas que ceux ici recensés et encore, ceux-ci ne sont-ils jamais « imposés » par la loi);

— lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de télécommunications;

— lorsque les actes sont posés en vue de permettre l'intervention des services de secours et d'urgence en réponse aux demandes d'aide qui leur sont adressées.

(204) La Cour n'a en effet pas censuré les écoutes administratives telles qu'organisées en droit allemand dans l'affaire *Klass* alors que, à supposer qu'il soit suffisamment accessible et prévisible au sens de la Convention, l'article 259^{bis} du Code pénal belge n'autorise que les écoutes administratives du SGR, et d'aucune autre autorité administrative belge ou étrangère, écoutes qui ne peuvent être effectuées qu'à l'étranger (ce qui pose aussi le problème de l'extra-territorialité) et seulement à des fins strictement militaires.

autorités belges qu'à celles des Etats participant à Echelon qui doivent respecter la souveraineté territoriale (205).

De toute façon, à supposer qu'existe une loi applicable, qu'elle puisse de surcroît être appliquée en-dehors du territoire des Etats à partir desquels l'interception est effectuée et qu'elle puisse passer outre aux prohibitions portées par le droit des Etats sur le territoire desquels elles ont lieu, Echelon ne s'en exposerait pas moins à des critiques fondamentales en raison du manque de « prévisibilité » et d'« accessibilité » des normes qui régiraient son fonctionnement.

2. Les exigences tenant lieu à la qualité de la « loi »

a. Les principes généraux relatifs à la qualité de la « loi »

36. La jurisprudence *Sunday Times* et *Leander* — La condition de légalité est rencontrée dès lors que le droit interne, quand il permet les écoutes, sous réserve des principes inhérents à la souveraineté des États tiers, est suffisamment accessible et prévisible (206).

On ne peut ici que rappeler l'attendu de principe posé par la Cour européenne des droits de l'homme dans l'arrêt *Sunday Times* et qu'elle a constamment rappelé depuis lors à propos de chaque disposition de la Convention qui prévoit qu'une ingérence dans un droit garanti doit être « prévue par la loi » :

« il faut d'abord que la 'loi' soit suffisamment accessible : le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné. En second lieu, on ne peut considérer comme une » loi « qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé. Elles n'ont pas besoin d'être prévisibles avec une certitude absolue : l'expérience la révèle hors d'atteinte. En outre la certitude, bien que hautement souhaitable, s'accompagne parfois d'une rigidité excessive. Or le droit doit pouvoir s'adapter aux changements de situation. Aussi beaucoup de lois se servent-elles, par la force des choses, de formules plus ou moins vagues dont l'interprétation et l'application dépendent de la pratique » (207).

(205) Cette interprétation est également celle du lieutenant — général MICHAUX, commandant du SGR, le service général de renseignement de l'armée. En effet, le quotidien *De Morgen* du 12 mai 2000 écrit : « Volgens generaal Michaux zou het volgen van een systeem zoals Echelon zelfs 'illegaal' zijn in België, 'gelet op het ontbreken van een wetgeving in dit land inzake veiligheidsintercepties' ». Néanmoins, Mme TIMMERMANS, nouvelle Administratrice générale de la Sécurité de l'Etat, vient de plaider pour l'instauration légale des écoutes administratives (*La Libre Belgique* 16.06.2000).

(206) Pour un exemple où la Commission estime ces qualités rencontrées en matière d'écoutes : déc. 30 novembre 1994, *K.D. c. Pays-Bas*, req. n° 21207/93, *D.R.* 79-A, p. 31.

(207) Arrêt *Sunday Times c. Royaume Uni* du 26 avril 1979, § 49.

Les principes d'accessibilité et de prévisibilité, s'ils ne sauraient avoir une portée absolue, n'en revêtent pas moins une importance majeure en ce qu'ils soutiennent le principe encore plus fondamental de la prééminence du droit.

La Cour a également précisé que

« l'un des principes sous-jacents à la Convention, la prééminence du droit, veut qu'une immixtion des autorités dans les droits d'un individu puisse subir un contrôle efficace. Il en est spécialement ainsi lorsque (...) la loi investit l'exécutif d'amples pouvoirs discrétionnaires dont l'exercice relève d'une pratique sujette à évolution mais échappant à tout examen du Parlement » (208).

L'arrêt *Leander contre Suède* du 26 mars 1987, cité en exergue du présent article, est exemplaire de la manière dont la Cour appréhende la « qualité » requise de la « loi » en cas d'ingérence secrète dans la vie privée :

« Dans le contexte particulier de contrôles secrets du personnel affecté à des secteurs touchant à la sécurité nationale, l'exigence de prévisibilité ne saurait cependant être la même qu'en maints autres domaines. (...) Néanmoins, dans un système applicable à tous les citoyens, (...) la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète et virtuellement dangereuse, dans leur vie privée. Pour s'assurer du respect du critère de prévisibilité, il faut tenir compte aussi des instructions ou des pratiques administratives n'ayant pas force de loi, pour autant que les intéressés les connaissent suffisamment » (209).

Rien ne s'oppose à ce que ces principes généraux soient invoqués à l'égard d'Etats participant à Echelon.

b. Echelon contre l'exigence de « la prévisibilité de la loi »

1° Le cas des écoutes téléphoniques

37. L'élaboration progressive d'un corpus jurisprudentiel minimal pour les écoutes — La jurisprudence de la Cour européenne des droits de l'homme a fréquemment censuré des dispositions internes ne répondant pas à ces exigences, en particulier sur le terrain de l'article 8 de la Convention, et à plusieurs reprises à propos d'écoutes téléphoniques. En effet, la prévisibilité de la norme a plusieurs fois fait défaut dans des affaires d'écoutes soumises à la Cour.

L'arrêt *Malone* qui concernait l'écoute par la police anglaise d'un anti-quaire soupçonné de recel d'objets volés, sur mandat du Ministre de l'Intérieur, a recherché

(208) Arrêt *Silver et autres c. Royaume Uni* du 25 février 1983, § 90.

(209) § 51 de l'arrêt *Leander* du 26 mars 1987. C'est nous qui soulignons.

« si le droit interne énonçait les éléments essentiels [du] pouvoir [d'interception] avec une précision raisonnable, des normes juridiques accessibles qui indiquaient suffisamment l'étendue et les modalités d'exercice du pouvoir d'appréciation attribué aux autorités compétentes » (210).

L'article 8 était violé en raison d'une ambiguïté et d'une incertitude telles que

« la Cour ne [pouvait] pas dire avec l'assurance souhaitable à quels égards le pouvoir d'interception se trouve intégré à des normes juridiques et sous quels rapports il reste tributaire de l'exécutif » (211).

C'est aux termes d'un examen approfondi et circonstancié que la Cour a conclu dans les affaires *Huvig contre France* et *Kruslin contre France* que les écoutes téléphoniques opérées par un officier de police judiciaire commis rogatoirement par un juge d'instruction avaient bien une base légale en droit français. La Cour s'est dans un premier temps refusée à suivre les requérants qui estimaient que le code de procédure pénale ne pouvait fonder les écoutes; elle a en effet estimé ne pas être habilitée à exprimer un point de vue contraire à la position constante des juridictions françaises, compétentes au premier chef pour interpréter et appliquer le droit interne. Néanmoins, faisait défaut l'exigence de prévisibilité. Pour arriver à ce constat, la Cour a bien du se livrer à un contrôle abstrait, jusqu'à un certain degré, de la « loi » en vigueur à l'époque des faits. Ces deux arrêts ont affirmé les principes applicables aux écoutes téléphoniques en estimant que

« les écoutes et autres formes d'interceptions des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. Partant, elles doivent se fonder sur une 'loi' d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner » (212).

Malgré certaines règles, et pas des moindres, imposées par la Cour de cassation française sur base du Code de procédure pénale (nécessité d'un mandat du juge d'instruction; contrôle que lui exerce sur la police judiciaire et contrôles juridictionnels sur ses propres décisions; interdiction des artifices et stratagèmes; obligation de confidentialité des conversations avec l'avocat de l'intéressé), d'autres règles avancées par le Gouvernement avaient des fondements moins clairs. Mais la Cour a surtout noté l'absence de délimitation préalable des infractions pouvant donner lieu à écoutes, l'absence de limitation dans le temps, de conditions d'établissement des procès-verbaux, de définition des principes d'effacement des bandes, etc. Bref, des sauvegardes adéquates contre divers abus faisaient défaut, entraînant par là violation de l'article 8 de la Convention. La France a adopté en consé-

(210) Arrêt *Malone c. Royaume Uni* du 27 juin 1984, § 70.

(211) Arrêt *Malone*, § 79. La conclusion fut identique à propos du comptage des conversations téléphoniques puisque n'existait « aucune norme juridique relative à l'étendue et aux modalités d'exercice du pouvoir d'appréciation dont jouissent les autorités » (§ 88).

(212) Arrêts *Huvig* et *Kruslin* du 24 avril 1990, respectivement § 32 et 33.

quence la loi du 10 juillet 1991 sur le secret des correspondances émises par la voie des télécommunications que la Cour a qualifiée comme énonçant désormais « *a priori* » avec suffisamment de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités (213).

La Cour est arrivée à la conclusion de la violation de l'article 8 dans l'arrêt *Kopp contre Suisse* puisque, malgré l'existence de plusieurs garanties procédurales, il y avait contradiction entre une loi claire qui protégeait le secret professionnel de l'avocat surveillé en tant que tiers et la pratique suivie qui avait, notamment, consisté à confier l'écoute ordonnée par le procureur général de la Confédération à un fonctionnaire des PTT, sans contrôle d'un magistrat indépendant (214).

38. Ce corpus tient désormais lieu de principes généraux applicables à toutes les écoutes téléphoniques — Dans une autre affaire, il a été jugé que, même si intervient entre l'écoute litigieuse et l'arrêt de la Cour une évolution législative et jurisprudentielle qui améliore le droit interne,

« [manquaient] notamment la définition des catégories de personnes susceptibles d'être mises sur écoute judiciaire, la nature des infractions pouvant y donner lieu, la fixation d'une limite à la durée de l'exécution de la mesure, les conditions d'établissement des procès-verbaux de synthèse consignant les conversations interceptées, et l'utilisation et l'effacement des enregistrements réalisés » (215).

L'arrêt *Valenzuela Contreras contre Espagne* du 30 juillet 1998 présente ainsi cet immense intérêt d'avoir intégré parmi les principes généraux appliqués par la Cour en matière d'écoutes téléphoniques les garanties procédurales dont l'absence avait motivé aussi la condamnation de la France dans les affaires *Huvig* et *Kruslin*.

L'affaire *Amann contre Suisse*, jugée le 16 février 2000, constitue pour sa part un cas d'école. D'abord parce que l'arrêt se réfère en tous points à la jurisprudence *Malone* sur les exigences particulières de prévisibilité qui doivent s'attacher aux écoutes secrètes menées par le pouvoir exécutif. Mais surtout parce que les faits de la cause sont très proches de ce que tout un chacun peut connaître du cas *Echelon*.

En effet, l'écoute litigieuse ainsi que l'établissement subséquent d'une fiche la relatant remontaient à 1981. L'écoute et la fiche concernaient un commerçant, concessionnaire d'appareils dépilatoires (!), qui avait été contacté téléphoniquement par une femme depuis l'ambassade soviétique. Ce n'est cependant qu'en 1990 que le public eut vent de l'existence d'un

(213) Arrêt *Lambert c. France* du 24 août 1998, § 28.

(214) Arrêt *Kopp c. Suisse* du 25 mars 1998, §§ 73-74. Cons. également l'opinion concordante du juge Pettiti sous l'arrêt qui constate que, malgré 20 ans de jurisprudence strasbourgeoise et une multitude de rapports nationaux et internationaux, les écoutes se poursuivent souvent dans l'arbitraire le plus complet et que s'y joignent les pratiques privées d'espionnage industriel.

(215) Arrêt *Valenzuela Contreras c. Espagne* du 30 juillet 1998, §§ 46 et 59.

fichier du ministère public consignait les résultats des demandes de renseignements adressées aux services de renseignement des polices cantonales; le requérant, parmi d'autres personnes, put alors consulter sa fiche pendant qu'étaient adoptées diverses mesures législatives.

La Cour a commencé par relever que l'arrêté du Conseil fédéral du 29 avril 1958 concernant le Service de police du ministère public fédéral habilitait celui-ci à procéder à des « *mesures de surveillance* » pour assurer « *le service des enquêtes et des informations dans l'intérêt de la sûreté intérieure et extérieure de la Confédération* ». Mais,

« [cet arrêté] ne contient aucune indication relative aux personnes susceptibles de faire l'objet de telles mesures, aux circonstances dans lesquelles celles-ci peuvent être ordonnées, aux moyens à employer ou aux procédures à observer ».

Partant,

« cette norme ne saurait en conséquence être considérée comme suffisamment claire et détaillée pour assurer une protection appropriée contre les ingérences des autorités dans le droit du requérant au respect de sa vie privée et de sa correspondance » (216).

Quant au Code de procédure pénale, il contenait certes plusieurs garanties comme la définition des catégories de personnes susceptibles d'être écoutées, la limitation dans le temps des écoutes, le contrôle d'un magistrat indépendant; mais le Gouvernement ne put établir si elles avaient été appliquées. En outre,

« la loi fédérale sur la procédure pénale vise avant tout la surveillance des personnes suspectées ou inculpées d'un crime ou d'un délit, voire les tiers présumés recevoir ou transmettre des informations à ces dernières, mais ne réglemente pas de façon détaillée le cas des interlocuteurs écoutés 'par hasard', en qualité de 'participants nécessaires' à une conversation téléphonique enregistrée par les autorités en application de ces dispositions. En particulier, la loi ne précise pas les précautions à prendre à leur égard » (217).

Faute de prévisibilité du droit qui lui était applicable, l'écoute violait donc l'article 8.

L'ensemble de ces précédents peut, sans conteste, être valablement invoqué à l'égard du programme Echelon qui résulte d'accords secrets passés entre Etats participants.

2° Le cas de la mémorisation de renseignements

39. L'identité de la protection de principe en cas d'écoutes téléphoniques et de tenue de bases de données — Les recommandations du Comité des Ministres du Conseil de l'Europe en matière de tenue des

(216) Arrêt *Amann c. Suisse* du 16 février 2000, § 58.

(217) Arrêt *Amann*, § 61. C'est nous qui soulignons ce passage qui peut également concerner directement Echelon.

registres de données par la police sont particulièrement explicites puisqu'elles demandent aux Etats Parties de s'inspirer de la jurisprudence de la Cour relative aux écoutes (218).

La Cour a également établi dans l'affaire *Amann* la violation de l'article 8 de la Convention tant en ce qui concerne l'établissement que la conservation de la fiche de renseignement qui avait résulté de l'écoute téléphonique. L'établissement d'une fiche mémorisée, qu'elle contienne ou non des éléments sensibles, que les informations qu'elle contient soient utilisées ou non, constitue en soi une ingérence. Sans même se pencher sur l'existence d'une « loi », dans la mesure où déjà le droit suisse ne prévoyait pas expressément l'existence du registre du ministère public, la Cour a constaté que les directives du Conseil fédéral ne contenaient aucune indication appropriée sur l'étendue et les modalités d'exercice des prérogatives du ministère public. Quant à la conservation de la fiche, la Cour a également remarqué que les renseignements mémorisés n'avaient pas été détruits alors qu'il était avéré qu'aucune infraction n'était en cours de préparation. Dans les deux cas, l'article 8 de la Convention a été violé puisque le droit suisse n'indiquait pas avec assez de clarté l'étendue et les modalités du pouvoir des autorités (219).

Les mêmes principes furent appliqués à la conservation de données par les services de renseignement dans l'arrêt *Rotaru* du 4 mai 2000 qui condamna la Roumanie car

« aucune disposition du droit interne ne fixe les limites à respecter dans l'exercice de ces prérogatives. Ainsi, la loi interne ne définit ni le genre d'informations pouvant être consignés, ni les catégories d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet de mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre. De même, la loi ne fixe pas des limites quant à l'ancienneté des informations détenues et la durée de leur conservation » (220).

Les arrêts *Amann* et *Rotaru*, qui font suite à l'arrêt *Leander*, appliquent par conséquent à la conservation des données exactement les mêmes règles que celles qui prévalent à l'encontre des écoutes téléphoniques, ce qui est déterminant pour contester Echelon. Tant en amont (dès la décision d'écoute, en fait laissée à la discrétion d'ordinateurs qui intercepteraient

(218) L'exposé des motifs de la Recommandation précitée n° R (87) 15 précise ainsi en son § 47 que « les organes de répression exercent leurs fonctions dans les limites de la loi et leurs activités de collecte des données sont restreintes en conséquence. Il y a donc lieu de respecter les dispositions du droit interne, qui doivent avoir pour base minimale les clauses de la Convention (...). A cet égard, on doit tenir compte également de la jurisprudence (...) dans les domaines de l'arrestation ou de la détention pour interrogatoire, des perquisitions et saisies, des méthodes d'interrogatoire, des prélèvements sur le corps humain, des empreintes digitales et photographies, etc. Il va sans dire que la législation interne pertinente doit être conforme aux dispositions de la Convention, telles qu'interprétées par la Cour européenne des droits de l'homme ».

(219) Arrêt *Amann*, §§ 75 à 80.

(220) Arrêt *Rotaru* du 4 mai 2000, § 57.

tous types de messages par voie électronique), qu'en aval (lors du traitement après triage éventuel de ce qui est pertinent pour les services des pays participants), l'article 8 de la Convention européenne des droits de l'homme a bel et bien vocation à en réagir le moindre rouage.

Cette conclusion est d'autant plus confortée que, dans un autre contentieux dont elle a également eu à connaître à plusieurs reprises, à savoir celui de la compatibilité avec l'article 8 des mesures d'interception de la correspondance des détenus, la juridiction strasbourgeoise a condamné la Pologne ce 4 juillet 2000 en raison du manque de prévisibilité de sa législation. Celle-ci permettait en effet la censure automatique du courrier des détenus par les autorités pénales, en ce comprises les lettres échangées avec un médiateur. Le constat de violation opéré par la Cour est très éclairant :

« the applicable provisions did not draw any distinction between the different categories of persons with whom the prisoners could correspond. Consequently, also the correspondence with the Ombudsman was subject to censorship. Moreover, the relevant provisions had not laid down any principles governing the exercise of this censorship. In particular, they failed to specify the manner and the time-frame within which it should be effected. As the censorship was automatic, the authorities were not obliged to give a reasoned decision specifying grounds on which it had been effected » (221).

Saisies indifférenciées, absence de limitation temporelle, inexistence de la motivation de la censure,... sont également autant de manquements pouvant raisonnablement être adressés à Echelon.

c. Echelon contre l'exigence de « l'accessibilité de la loi »

40. Le manque de publicité des éventuelles règles juridiques relatives à Echelon, un manquement manifeste à l'article 8 de la Convention — A supposer remplies conditions tenant à la prévisibilité des normes suivies dans le cadre du programme Echelon, ce qui laisse planer un doute certain (222), notamment en raison de la pluralité de droits nationaux potentiellement applicables, on pourrait de toute façon difficilement soutenir que ces divers droits nationaux, à les supposer valablement applicables à des personnes qui ne résident pas sur le territoire et qui ne sont pas ressortissantes des États parties au programme, répondent, ensemble ou séparément, aux exigences d'accessibilité.

L'adage '*Nul n'est censé ignorer la loi*' (même lorsque l'on s'entoure de « conseils éclairés ») tient déjà largement lieu de fiction dans un ordre juridi-

(221) Arrêt *Niedbala c. Pologne* du 4 juillet 2000, § 81. La condamnation des saisies indifférenciées de correspondance d'un failli, notamment en ce qui concerne les courriers échangés avec son avocat, a été opérée par l'arrêt *Foxley c. Royaume Uni* du 20 juin 2000, § 43, non lors du contrôle de « légalité » mais lors du contrôle de « nécessité ».

(222) Cf. notamment la section 309 de l'*Intelligence Authorization Act for Fiscal Year 2000*, citée dans l'introduction, que le Congrès américain a du adopter pour forcer la N.S.A. à dévoiler sur quelles bases légales elle procède à des écoutes et interceptions.

que national. Que dire alors lorsque l'on est surveillé en fonction de règles relevant d'un ou plusieurs ordres juridiques étrangers dont, pour peu qu'elles existent, on ne soupçonne même pas l'existence (223)? Justement parce que cette surveillance est secrète...

Le 12 mai 2000 est, à cet égard, une date à marquer d'une pierre blanche dans l'histoire de la jurisprudence strasbourgeoise puisque c'est pour la première fois, à notre connaissance, que la Cour européenne des droits de l'homme a condamné un Etat pour faute d'accessibilité de sa législation et ce, qui plus est, dans une affaire d'écoutes téléphoniques. La Cour avait jusque là fait preuve de mansuétude, ayant encore estimé huit jours auparavant que la publication d'une loi dans le Journal Officiel du pays concerné suffisait à la rendre « accessible » au sens de la Convention (224). Mais, comme le laissait déjà entrevoir un rapport adopté le 14 janvier 1998 par l'ancienne Commission, le droit anglais, puisque c'est de lui qu'il s'agit, ouvrait ouvertement le flanc à la critique en ce que les circulaires du Home Office sur la mise en œuvre du *Police and Criminal Evidence Act* de 1984 souffraient d'un déficit de publicité avéré (225).

L'arrêt *Khan contre Royaume Uni* avait à se prononcer sur l'interception des conversations téléphoniques d'une personne soupçonnée de trafic de drogue, la production d'enregistrements ayant entraîné sa condamnation en justice. Les circulaires du Home Office n'étaient consultables qu'à la bibliothèque du Parlement, ce qui entraînait la violation subséquente de l'article 8 de la Convention :

« At the time of the events in the present case, there existed no statutory system to regulate the use of covert listening devices, although the Police Act 1997 now provides such a statutory framework. The Home Office Guidelines at the relevant time were neither legally binding nor were they directly publicly accessible. The Court also notes that Lord Nolan in the House of Lords commented that under English law there is, in general, nothing unlawful about a breach of privacy. There was, therefore, no domestic law regulating the use of covert listening devices at the relevant time » (226).

Cette exigence minimale de transparence administrative faisait défaut dans l'affaire *Khan* (227). Une fois de plus, que dire alors d'Echelon? Sur-

(223) Voyez également *infra* les considérations largement semblables exposées à propos de l'inapplicabilité du principe de l'épuisement des voies de recours internes.

(224) Arrêt *Rotaru c. Roumanie* du 4 mai 2000, § 54.

(225) Rapport de la Commission du 14 janvier 1998 établissant une violation de l'article 8, req. n° 27237/95, *Govell c. Royaume Uni*, § 62.

(226) Arrêt *Khan c. Royaume Uni* du 12 mai 2000, § 27. L'arrêt (seulement disponible en anglais), rendu par la troisième section, ne sera définitif qu'à l'expiration du délai de trois mois ouvrant recours devant la Grande Chambre.

(227) Sur la portée de la Convention dans le domaine de la transparence administrative en général, et de la publicité de l'action administrative en particulier : P. POPELIER, « De openbaa-
rheid van het overheidshandelen in het democratische rechtsstaat », *T.B.P.* 1995, p. 174; D. YER-
NAULT, « Libertés classiques et droits dérivés : le cas de l'accès aux documents administratifs », *R.T.D.H.* 1996, pp. 225.

tout si l'on sait que, le 5 juin 2000 encore, le Gouvernement britannique refusait toujours de communiquer au Parlement les accords secrets passés avec les Etats Unis quant à l'utilisation de la base de Menwith Hill (228).

d) *Une légitimité contestable : sécurité nationale, souveraineté territoriale et privatisation du fruit des interceptions*

41. Le contrôle de la légitimité des ingérences est très restreint ce qui ne signifie pas qu'il n'existe pas — Il est très rare que la Cour analyse en profondeur les griefs relatifs à la légitimité du but poursuivi par une ingérence. Dès lors que certains des motifs avancés par le Gouvernement défendeur cadrent avec ceux requis par la Convention, comme la sauvegarde de la sécurité nationale et/ou la défense de l'ordre et la prévention des infractions pénales, la Cour ne se prononce pas sur les autres motifs qui pourraient être avancés (229). Même si prévaut dans le contrôle de la légitimité par la Cour le principe d'interprétation restrictive, c'est-à-dire qu'aucun autre motif que ceux strictement énumérés au § 2 de l'article 8 ne peut être poursuivi, elle peut en avoir une conception assez large (230).

Mais la Cour a, par exemple, déjà mis en doute le but que pouvait bien poursuivre la divulgation par une décision judiciaire du nom et de l'état de santé d'une personne atteinte du SIDA (231). Elle a surtout émis de sérieux doutes quant à l'existence de l'objectif de sécurité nationale poursuivi par des investigations menées au sein des forces armées à l'encontre de militaires qui reconnaissaient leur homosexualité; l'article 8 ayant été violé faute de nécessité de ces mesures dans une société démocratique, la Cour n'a toutefois pas poursuivi son examen de la légitimité de telles ingérences (232).

Il est cependant douteux que le motif tiré de la préservation du « bien-être économique du pays » autorise valablement un Etat à procéder à des écoutes aux détriments d'entreprises commerciales étrangères pour en communiquer les fruits à certaines de ses entreprises pour faire gagner à celles-ci des marchés. Si ce motif, ainsi que celui tiré de « la protection des droits et libertés d'autrui », justifie certainement qu'un Etat réglemente la concurrence et restreigne, par exemple, la liberté d'expression notamment dans le

(228) *Supra*, n° 8.

(229) Ainsi, dans l'arrêt *Klass* du 4 juillet 1978, des motifs tirés de la sécurité des forces alliées stationnées en R.F.A. ou, à l'époque des faits, de celle des troupes de l'une des trois puissances alliées se trouvant dans le Land de Berlin, n'ont pas été expressément analysés (§§ 45-46).

(230) Par exemple, de manière tout à fait logique, elle a englobé dans la notion de « bien-être économique du pays » l'obligation de communiquer des renseignements médicaux car une telle obligation est potentiellement décisive pour l'allocation de fonds publics à des demandeurs remplissant les critères d'octroi : arrêt *M.S. c. Suède* du 27 août 1997, § 38.

(231) Arrêt *Z. c. Finlande* du 25 février 1997, §§ 77 et 78. La Cour ne s'est toutefois pas prononcée sur la violation de l'article 8 à ce stade de l'examen dans la mesure où elle a par la suite établi que la divulgation n'était pas nécessaire dans une société démocratique.

(232) Arrêt *Smith et Grady c. Royaume Uni* du 27 septembre 1993, § 74.

domaine de la publicité commerciale (233), cela ne l'habilite nullement à violer les principes les plus élémentaires du droit de la concurrence institué dans le cadre de l'Union Européenne, de l'Espace Économique Européen, de l'O.C.D.E. ou encore de l'O.M.C.. Que se soit au détriment de la politique économique d'autres Etats, d'entreprises ou des activités commerciales de particuliers. Or, le rapport « *Campbell* » fait largement état d'informations selon lesquelles certaines sociétés américaines auraient bénéficié des fruits d'interceptions menées dans le cadre d'Echelon pour arracher des marchés face à des concurrentes. Les cas de communication de renseignements collectés par la police à des personnes privées ne peuvent être qu'exceptionnels (234).

Quant aux motifs d'ingérence dans la vie privée reposant sur la « sécurité nationale », un État pourrait les contester dans la mesure où il n'appartient pas à l'État qui procède à des écoutes d'imposer en-dehors de ses frontières sa propre conception de cette sécurité.

Les principes directeurs relatifs aux fichiers électroniques de données personnelles que l'Assemblée générale de l'O.N.U. a fait siens dans une résolution du 14 décembre 1990 qui s'adresse tant aux Gouvernements qu'aux Organisations internationales et aux organisations non gouvernementales peuvent également faire office de balises en la matière. Ainsi, le premier de ces principes, dit principe de légalité et de loyauté (« *principle of lawfulness and fairness* »), dispose que

« informations about persons should not be collected or processed in unfair or unlawful ways, nor should be used for ends contrary to the purposes and principles of the Charter of the United Nations » (235).

Et parmi ces principes portés par l'article 2 de la Charte figure la souveraineté territoriale.

L'arrêt *Rotaru c. Roumanie* du 4 mai 2000 a estimé que les motifs invoqués pour justifier le fichage par les services de renseignement n'étaient pas définis avec suffisamment de précision mais a préféré exercer malgré tout le contrôle traditionnel de « prévisibilité » (236). L'opinion concordante du juge Widhaber, à laquelle se sont ralliés les juges Makarczyk, Türmen, Costa, Tulkens, Casdevall et Weber, a critiqué cette timidité en affirmant, ce qui s'applique pleinement à Echelon, que

(233) L. BOISSON DE CHAZOURNES, « Publicité commerciale et liberté d'expression dans le cadre du Conseil de l'Europe », *R.G.D.I.P.* 1988, pp. 929-960; G. COHEN-JONATHAN, « Liberté d'expression et message publicitaire », *R.T.D.H.* 1993, p. 69; C. GOUX, « L'interdiction de certaines formes de publicité et la Convention européenne des droits de l'homme », *L'Ingénieur-conseil* 1991, pp. 319-345, ... et surtout M. DE MERIEUX, « The German Competition Law and article 10 ECHR », *Eur. Law Rev.* 1995, pp. 388-399.

(234) Voyez les conditions très restrictives portées par le point 5.3.1. de la Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adressée le 17 septembre 1987 par le Comité des Ministres du Conseil de l'Europe.

(235) A/RES/45/95.

(236) § 58 de l'arrêt *Rotaru*.

« expliquer que la conservation, pour ainsi dire sans discernement, d'informations relatives à la vie privée d'individus correspond à un souci légitime de sécurité nationale pose manifestement problème » (237).

L'existence d'Echelon peut dès lors poser de sérieuses questions de « légitimité » au regard de l'article 8 de la Convention, sachant que la Cour européenne des droits de l'homme donne certains signes, encore timides certes, de sa volonté de contrôler la pertinence des motifs de sécurité nationale invoqués pour justifier les mesures de surveillance secrète.

e) *Une nécessité outrepassée : le caractère « global » des interceptions électroniques et le déficit de garanties procédurales*

1. *L'analyse classique de la nécessité d'une ingérence dans une société démocratique : Echelon contre l'interdiction des écoutes exploratoires et générales*

42. La large marge d'appréciation dont jouissent les Etats en matière de sécurité nationale ne saurait signifier pouvoir arbitraire — La notion de nécessité implique que l'ingérence corresponde à un besoin social impérieux et qu'elle soit, en particulier, proportionnée au but légitime poursuivi (238). La jurisprudence, parfois flottante, de la Cour européenne des droits de l'homme sur la marge d'appréciation dont disposent les autorités nationales pour établir la nécessité des ingérences dans les droits garantis par la Convention est connue (239).

Il est bien établi que cette nécessité est analysée à l'aune de l'ensemble de l'affaire soumise. Certaines restrictions trop générales au droit de correspondre des détenus ont été déclarées en contradiction avec l'article 8 (240). Dans une affaire portant sur la transmission d'un dossier médical, et ayant eu égard aux autres instruments de protection développés par le Conseil de l'Europe, la Cour a affirmé qu'elle tenait compte du

« rôle fondamental que joue la protection des données à caractère personnel (...) pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention » (241).

(237) Opinion concordante e.a. du juge WILDHABER sous l'arrêt *Rotaru* du 4 mai 2000.

(238) Pour un exemple, parmi beaucoup d'autres, rappelant la jurisprudence de la Cour : Comm.eur.d.h., déc. du 16 avril 1998, req. n° 31513/96, *Hildebrand c. Allemagne*, « <http://www.dhcour.coe.fr/Hudocldoc/hedec/sift/4047.txt> », p. 4 sur 7.

(239) E. KASTANAS, *Unité et diversité : notions autonomes et marge d'appréciation des Etats dans la jurisprudence de la Cour européenne des droits de l'homme*, Bruxelles, Bruylant, 1996. Pour une critique du manque de lisibilité de cette jurisprudence : S. van DROOGHENBROECK, « Conflits entre droits fondamentaux et marge nationale d'appréciation », *J.T.D.E.* 1999, p. 162. Le contrôle opéré par le Comité des droits de l'homme dans le cadre de l'article 17 du P.I.D.C.P. consiste à apprécier, vu la prohibition des immixtions illégales et arbitraires que porte cette disposition, si l'immixtion peut être « raisonnable dans les circonstances » (décision du 29 juillet 1997, com. n° 549/1993, *Hopu et Bessert c. France*, point 10.3).

(240) Arrêt *Silver c. Royaume Uni* du 25 février 1983, § 99.

(241) Arrêt *Z. c. Finlande* du 25 février 1997, § 95.

La marge d'appréciation des États est certainement plus grande lorsqu'est invoquée la sécurité nationale mais n'empêche pas son contrôle par la Cour européenne des droits de l'homme.

Dans l'affaire *Klass*, la Cour avait commencé par prendre acte de l'évolution des progrès techniques en matière de surveillance ainsi que du développement du terrorisme et de formes très complexes d'espionnage. La nécessité des écoutes dans le contexte qui était celui de l'Allemagne en 1978 n'était pas contestée. Cet arrêt, qui traitait, il convient de le souligner, d'écoutes administratives, fut toutefois l'occasion d'affirmer certains principes fondamentaux sur la manière dont les États peuvent employer la marge d'appréciation qui leur est reconnue :

« quant au choix des modalités du système de surveillance, la Cour relève que le législateur national jouit d'un certain pouvoir discrétionnaire. Elle n'a sûrement pas qualité pour substituer à l'appréciation des autorités nationales une autre appréciation de ce que pourrait être une autre politique en ce domaine (...). La Cour souligne néanmoins que les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée ».

La relativité de l'appréciation par la Cour est en outre affaire de contexte :

« quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne » (242).

Les garanties existant en l'espèce étaient en conformité avec l'article 8 de la Convention. Leur énumération peut donner de quoi réfléchir. Quant au fond, les conditions légalement en vigueur étaient les suivantes : existence d'indices se rapportant à l'éventualité de la commission d'infractions graves, seulement en cas d'échec d'autres modes de preuve, limitation aux seuls contacts du suspect,... Quant à la procédure : uniquement sur demande écrite et motivée, demande ne pouvant être formulée que par certains chefs de service, décision n'appartenant qu'au Ministre compétent, sollicitation en pratique de l'autorisation préalable de la commission parlementaire apte à se prononcer sur les recours, etc. (243).

(242) Arrêt *Klass c. Allemagne* du 4 juillet 1978, §§ 49 et 50.

(243) Voyez également l'arrêt *Leander* du 26 mars 1987, §§ 63-67 en ce qui concerne les garanties que présentaient le droit suédois, notamment les contrôles opérés par l'ombudsman et la Commission parlementaire de Justice.

Ainsi, les garanties de légalité et de proportionnalité offertes par le droit anglais (les *Interception of Communications Act* de 1985 et *Secret Service Act* de 1989 ont notamment mis en place un Tribunal pour les interceptions de communications et un Tribunal pour les services secrets) ont bel et bien été reconnues en conformité avec l'article 8 de la Convention mais il s'agissait, *in casu*, de l'interception des fax adressés ou reçus par un syndicaliste anglais sur le territoire national avec des syndicats d'Europe de l'Est (244).

43. Le caractère exploratoire et général prêté à un système de surveillance comme Echelon entraîne également une violation manifeste de l'article 8 de la Convention — Dans l'affaire *Miailhe n° 1*, était en cause une violation du droit au domicile, également garanti par l'article 8 de la Convention, en raison de fouilles et perquisitions douanières. La Cour formula l'observation particulière suivante en établissant la violation :

« les saisies subies par M. et Mme Miailhe revêtirent un caractère massif et surtout indifférencié; à telle enseigne que les douanes jugèrent sans intérêt pour l'enquête plusieurs milliers de documents et les restituèrent aux intéressés » (245).

C'est ainsi le caractère indifférencié de la lecture préalable par un liquidateur de faillite de toute la correspondance d'un failli, en ce compris les courriers échangés avec son avocat, qui a justifié la condamnation du Royaume Uni dans le récent arrêt *Foxley* (246).

On rappellera par ailleurs que dans l'affaire *Klass*, la circonstance que

« la législation incriminée n'autorise pas une surveillance dite exploratoire ou générale »

avait déjà pesé d'un poids certain dans l'appréciation par la Cour de la conformité du système allemand d'écoutes administratives (247).

La conférence des commissaires européens à la protection des données instituée par l'article 29 de la Directive 95/46/CE a également souligné cette prohibition par la Cour européenne des droits de l'homme de toute

(244) Comm., déc. du 27 juin 1994, *Christie c. Royaume-Uni*, req. n° 21482/93, D.R. 78-A, p. 119, ainsi que les affaires y citées à propos du *Secret Service Act*. On notera que cette décision d'irrecevabilité pour défaut manifeste de fondement est motivée de façon exceptionnellement détaillée et que la Commission n'avait peut-être pas conscience, à l'époque, de ce dont il s'agissait réellement puisque c'est la décision dans laquelle est mentionnée l'existence du « Dictionary ».

(245) Arrêt *Miailhe n° 1 c. France* du 25 février 1993, § 39.

(246) Arrêt *Foxley c. Royaume Uni* du 20 juin 2000, § 43. Il est rappelé que la censure indifférenciée du courrier des détenus peut aussi entraîner violation de l'article 8 comme cela fut jugé dans l'arrêt *Niedbala c. Pologne* du 4 juillet 2000 dans le cadre du contrôle de « légalité » et de « prévisibilité ».

(247) Arrêt *Klass c. Allemagne* du 4 juillet 1978, § 51. Adde à propos de la jurisprudence américaine qui emporte le caractère illicite des surveillances ou investigations systématiques ou collectives non motivées par un soupçon particulier : F. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles et Paris, Bruylant et L.G.D.J., 1990, p. 427.

surveillance exploratoire ou générale des télécommunications à grande échelle (248).

De surcroît, l'Observation générale n° 16 du Comité des Droits de l'Homme de l'O.N.U. insiste aussi particulièrement pour que les ingérences dans le droit au respect de la vie privée et de la correspondance, que les écoutes soient administratives ou judiciaires, n'interviennent qu' « *au cas par cas* » (249).

C'est donc à bon droit que la Résolution de la Commission des Libertés du Parlement européen adoptée le 11 avril 2000 stigmatisait Echelon aux termes de considérations transposables pour tous les réseaux d'interception de ce genre (250).

Le caractère massif et indifférencié des écoutes et interceptions dont question dans le programme Echelon (251) peut ainsi se révéler en contradiction avec l'article 8 de la Convention (252), d'autant plus que les victimes de ces ingérences totalement disproportionnées, par rapport à un but dont la légitimité est par ailleurs contestée, sont quasiment non-identifiables. L'existence d'un tel système exploratoire et général d'interception, caractéristiques inhérentes au programme « Dictionary » qui serait le cœur même d'Echelon, outrepassa manifestement la marge, pourtant grande, dont les États jouissent en matière de sécurité nationale pour apprécier la nécessité de ces ingérences dans le droit au respect de la vie privée et de la correspon-

(248) Audition de M. THOMAS, président de la Commission belge de la protection de la vie privée, par la Commission de la Justice de la Chambre lors de l'examen du projet de loi sur la criminalité informatique, *Doc. parl.*, Chambre, s.o. 1999-2000, 50 0213/004, p. 32 (également p. 96), qui ajoute, en critiquant entre autres l'absence de délai de conservation des données saisies, qu' « *il ne faudrait pas en arriver à créer diverses banques de données distinctes et supplémentaires en application du fantasme qui veut que 'cela peut toujours servir un jour'.* »

(249) C.D.H., observation générale n° 16 précitée, §§ 4 et 8.

(250) Points L et N bis de la Résolution « Watson » précitée, adoptée le 11 avril 2000 par la Commission des Libertés du Parlement européen.

(251) Voyez notamment l'étude précitée de Vincent WRIGHT du 6 janvier 1998. Toutes les communications (ou tous les messages acheminés par telle technologie) seraient donc interceptées; ce n'est que dans un second temps que le filtrage serait opéré à l'aide des programmes « Dictionnaires » qui comportent les mots-clés, phrases, personnes et lieux dont l'identification est souhaitée par les services de renseignement de l'un des pays du système UKUSA.

(252) Comme le note G. COHEN-JONATHAN, « Les écoutes téléphoniques », *op. cit.*, p. 101, « la surveillance ne peut être exploratoire ou générale. Il faut qu'une personne soit suspectée d'avoir commis une action susceptible d'être instruite de cette façon. C'est pourquoi, l'autorisation d'effectuer des écoutes doit être motivée de manière précise et ne pourra viser qu'une seule poursuite à la fois. C'est pourquoi aussi ce 'système' ne peut être utilisé que si les moyens traditionnels d'enquête sont inopérants ou ont abouti à un échec ». En ce qui concerne plus particulièrement les écoutes administratives, il convient d'aménager un contrôle approprié contre tout abus (p. 102). Mais par hypothèse, ces contrôles ne peuvent être réputés accessibles aux particuliers qui ne relèvent ni de la juridiction territoriale, ni de la juridiction personnelle des États qui pratiquent ce genre d'écoutes. Également A. PATIJN, « Data protection in the police sector », in *La protection des données dans le secteur de la police*, séminaire du Conseil de l'Europe des 13-14 décembre 1999, Strasbourg, Conseil de l'Europe, ADACS/DGI (2000) 3 Sem, p. 24.

dance (253), à plus forte raison si les interceptions concernent des communications passées intégralement sur des territoires tiers. Echelon viole pour ainsi dire « en soi » l'article 8 (254).

2. *L'analyse nouvelle de la nécessité d'une ingérence dans une société démocratique : Echelon contre la dimension processuelle de l'article 8 de la Convention*

44. Le processus décisionnel débouchant sur une ingérence doit être 'équitable' — Même si la marge d'appréciation des Etats est grande en matière de sécurité nationale, pouvoir discrétionnaire ne saurait signifier non plus arbitraire sur le plan procédural. Les moyens mis en œuvre doivent être proportionnés et reposer sur des motifs pertinents et suffisants. La Cour a synthétisé les principes de sa jurisprudence dans l'arrêt *Buckley* :

« chaque fois que les autorités nationales se voient reconnaître une marge d'appréciation susceptible de porter atteinte au respect d'un droit garanti par la Convention (...), il convient d'examiner les garanties procédurales dont dispose l'individu pour déterminer si l'Etat défendeur n'a pas fixé le cadre réglementaire en outrepassant les limites de son pouvoir discrétionnaire. Selon la jurisprudence constante de la Cour, même si l'article 8 ne renferme aucune condition explicite de procédure, il faut que le processus décisionnel débouchant sur des mesures d'ingérence soit équitable et respecte comme il se doit les intérêts de l'individu protégés par l'article 8 » (255).

L'évolution de la jurisprudence de la Cour a donc fait que les droits substantiels renferment désormais également des droits processuels dont l'examen du respect fait partie intégrante du contrôle de nécessité dans une société démocratique (256). Ceci n'est guère étonnant puisque les écoutes,

(253) Le 6^e principe directeur de l'O.N.U. sur les fichiers informatiques de données personnelles autorise également des exceptions fondées sur la sécurité nationale ou l'ordre public mais pour peu que *« such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards »*.

(254) Que tous les messages électroniques ne soient pas interceptés est indifférent : il suffit, par exemple, que seules les conversations par satellite ou seulement certains types de messages émanant de certains types de personnes soient surveillées. Encore que, mise à part la communication par fibre terrestre, la plupart des supports de transmission puissent faire l'objet de captations systématiques. Ce qui est déjà condamnable en soi, c'est l'interception par sondage, la captation aveugle et indiscriminée, la simple quête d'indices « pour voir »,... Il suffit également, pour qu'il y ait violation de l'article 8, que tout message contenant certains mots-clés soit intercepté (qu'il y ait tri ou non, qu'il y ait utilisation ultérieure ou non de l'information captée,...) puisque dans la masse répondant à d'éventuels critères de sélection (lesquels ? avec quels recours ?), il serait douteux que chaque message soit bien constitutif d'une menace pour les intérêts vitaux des Etats Unis.

(255) Arrêt *Buckley c. Royaume-Uni* du 25 septembre 1996, § 76.

(256) Pour un exemple tiré de l'article 3 de la Convention qui impose une obligation d'enquête lorsque sont allégués des actes de torture : arrêt *Ihlan c. Turquie* du 27 juin 2000, § 89 et *infra* sur les obligations de vigilance. On note aussi le processus exactement inverse à propos des droits processuels qui comportent de plus en plus des aspects substantiels : *Les nouveaux développements du procès équitable au sens de la Convention européenne des droits de l'homme*, actes du colloque du 22 mars 1996 de la Cour de cassation de France et de l'Université Robert Schuman

non contentes de constituer une ingérence dans la vie privée, peuvent également gravement mettre en cause l'exercice des droits de la défense (257). La Cour a en effet connu plusieurs affaires sur l'admissibilité des écoutes téléphoniques comme mode de preuve dans le cadre de l'article 6 de la Convention qui garantit le droit à un procès équitable (258).

Il a été jugé dans les trois arrêts rendus le 25 février 1993 à propos des perquisitions douanières que celles-ci seraient en contrariété avec l'article 8 de la Convention si elles ne reposaient pas sur un mandat judiciaire (259). Et celui-ci doit aussi revêtir une certaine qualité, celle de sa précision (260).

45. Un principe également valable pour les écoutes administratives — Peut-on aller jusque là en ce qui concerne toutes les écoutes téléphoniques ? Il paraît certes difficile de soutenir que seules les écoutes judi-

de Strasbourg, Bruxelles, Bruylant, 1996. Le refus opposé à des catholiques en Irlande du Nord de soumissionner dans le cadre de marchés publics à la suite d'enquêtes de sécurité a été jugé de nature à nuire à leur réputation ; la Commission ayant constaté la contrariété d'une immunité de juridiction des services de sécurité avec l'article 6, qui garantit le droit à un procès équitable, n'a pas jugé utile d'analyser le litige sous l'angle de l'article 8 dans la mesure où le grief tenant lieu au manque de proportionnalité de la mesure invoquait des garanties procédurales déjà examinées à propos de l'article 6 : Comm.eur.d.h., rapport du 8 avril 1997, req. n° 20390/92 et 21322/93, *John Tinnely & Sons Ltd and others c. Royaume Uni*, § 107 (« <http://www.dhcour.coe.fr/Hudocldoc/herep/sift/508.txt> »).

(257) A ce sujet : D. GARABEDIAN, *op. cit.*, p. 734. *Adde* l'opinion concordante du juge PETTIT sous l'arrêt *Malone* du 27 juin 1984.

(258) Voyez notamment l'arrêt *Schenk c. Suisse* du 24 juin 1988, § 48 : un enregistrement, même illégalement effectué, ne vicie pas la procédure si la condamnation repose sur un ensemble d'autres preuves. Le tout récent arrêt *Jasper c. Royaume Uni* du 16 février 2000 a très fortement divisé la Grande Chambre, puisque c'est par 9 voix contre 8 qu'a été reconnu comme compatible avec le principe de l'égalité des armes la non-divulgaration d'éléments de preuve découlant d'une écoute. La Cour admet aussi la technique de l'infiltration d'agents de police opérant sous couverture secrète mais dans de strictes conditions (arrêt *Van Mechelen c. Pays-Bas* du 23 avril 1997, § 57). On doit cependant émettre de sérieuses réserves sur l'arrêt *Khan c. Royaume Uni* du 12 mai 2000 qui, bien qu'ayant estimé l'écoute téléphonique querellée en contrariété avec l'article 8, n'a pas vu de violation de l'article 6 dans le fait que cette écoute était pourtant le seul élément de preuve ayant entraîné la condamnation du requérant (§§ 37 et suiv.). Sous prétexte que l'ensemble de la procédure avait été équitable pour le reste, la Cour hypothèque singulièrement la portée du droit à un procès équitable, tout en s'écartant de la jurisprudence *Schenk* qui exigeait au moins qu'en la présence de preuves viciées, il devait exister d'autres éléments concordants justifiant la condamnation (voyez l'opinion concordante, en partie dissidente du juge LOUCAIDES).

(259) Arrêts du 25 février 1993, *Crémieux c. France* (§ 40), *Funke c. France* (§ 57), *Mialhe n° 1 c. France* (§ 38) : « l'administration des douanes disposait de pouvoirs fort larges : elle avait notamment compétence pour apprécier seule l'opportunité, le nombre, la durée et l'ampleur des opérations de contrôle. (...) En l'absence, surtout d'un mandat judiciaire, les restrictions et conditions prévues par la loi et soulignées par le Gouvernement apparaissaient trop lâches et lacunaires pour que les ingérences dans les droits des requérants fussent étroitement proportionnées au but légitime recherché ». Voyez D. YERNAULT, « Les pouvoirs d'investigation de l'administration face à la délinquance économique : les locaux professionnels et l'article 8 de la Convention européenne », *R.T.D.H.* 1994, pp. 121-136. L'arrêt *Camenzind c. Suisse* du 16 décembre 1997, §§ 45 à 47, constitue un malheureux retour en arrière dans la mesure où la Cour réautorise les perquisitions douanières sans mandat en raison des circonstances de l'espèce (protection forte du droit suisse, faiblesse de la perquisition). L'opinion dissidente d'un juge le conteste et l'opinion concordante de trois autres juges fait preuve de beaucoup de circonspection.

(260) Voyez à propos d'une perquisition opérée dans un cabinet d'avocat, l'arrêt *Niemietz* du 16 décembre 1992, § 37.

ciaires reposant sur un mandat seraient en conformité avec la Convention. En effet, la Cour a admis les écoutes administratives dont elle ne met pas en cause l'existence même. Ces dernières ne peuvent toutefois se dérouler non plus sous l'empire de l'arbitraire procédural le plus complet (261). À cet égard, le nombre impressionnant de garanties offertes par le système allemand analysé par la Cour dans l'affaire *Klass* constituait un ensemble qui, s'il n'avait été aussi détaillé, ne l'aurait sans doute pas conduite à admettre la validité des écoutes administratives. Plutôt que de soumettre le contrôle *a posteriori* des écoutes à un organisme judiciaire, l'Allemagne avait fait le choix du contrôle par un comité de cinq parlementaires, élu à la proportionnelle afin de garantir la représentation de l'opposition, comité doté de surcroît de pouvoirs et attributions suffisants (262).

Ce type de contrôle parlementaire ne paraît nullement exister dans le cadre du programme Echelon, du moins en ce qui concerne les personnes qui ne relèvent ni de la juridiction américaine, ni de la juridiction britannique (263). Un contrôle avoisinant est difficilement concevable vu la pluralité d'États qui y sont parties prenantes. Il ne semble pas exister d'organe commun de contrôle, ni qu'il y ait une quelconque indication renvoyant à un organe d'un État en particulier. D'ailleurs, lequel désigner? Celui de l'État à partir du territoire duquel a lieu l'interception? Un organe de l'État bénéficiaire de l'interception ou celui d'un État qui y procède effectivement par l'entremise de ses services de renseignement en action sur un territoire tiers? Confronté à de telles interrogations, on peut également douter plus que raisonnablement du respect de l'article 8 de la Convention.

Outre l'indépendance et l'effectivité requises du contrôle parlementaire, la Cour européenne des droits de l'homme a également constaté que, en vertu de la jurisprudence constitutionnelle allemande, l'intéressé devait être avisé, si pas immédiatement, du moins après la levée des mesures de surveillance dès que la notification de l'existence de celle-ci pouvait intervenir sans compromettre le but de la restriction au droit au respect de la vie pri-

(261) Ainsi, le rapport précité de Mr SCHMID d'avril 1999 pour la Commission des Libertés publiques du Parlement européen constatait de manière générale dans l'Union européenne ceci (p. 9) : « Il n'y a donc pas de réglementation européenne des écoutes téléphoniques, et plus généralement, de l'interception légale des télécommunications. Les réglementations nationales sont d'application. Au niveau national, les procédures prévoient, en principe, que ces écoutes téléphoniques (ou procédures comparables pour d'autres technologies que le téléphone) se font par la police sur la base de l'autorisation du Ministre compétent ou d'une commission rogatoire délivrée par un magistrat. Cette commission rogatoire impose des limites à l'action de la police (exemples : limites dans le temps, limites sur le type d'informations susceptibles d'être collectées) ».

(262) Arrêt *Klass*, §§ 52 à 57. Voyez cependant le point 2 de l'opinion séparée du juge PINHEIRO FARINHA qui estime que le principe de la séparation des pouvoirs s'accommode mal d'un contrôle politique des écoutes.

(263) Cette remarque est également valable en cas d'existence de tribunaux aptes à trancher les litiges relatifs aux interceptions de sécurité, ce qui est le cas au Royaume Uni et aux États Unis. Voyez plus loin à propos de l'épuisement des voies de recours internes (II.B.1.).

vée et de la correspondance (264). Or, il s'agissait bel et bien dans l'arrêt *Klass* de statuer sur des écoutes administratives (265).

Qui plus est, la jurisprudence de la Cour européenne des droits de l'homme portant sur l'exigence de prévisibilité de la « loi » en matière d'écoutes judiciaires peut aussi utilement, voire plus qu'ailleurs, soutenir l'argument tiré de l'absence de garanties procédurales suffisantes (266). Le droit communautaire a de son côté érigé en droit subjectif le recours juridictionnel pour les personnes qui ont des griefs à formuler à l'encontre de la manière dont sont collectées, traitées et conservées les données à caractère personnel qui les concernent (267).

Enfin, l'existence de recours, mêmes judiciaires et dûment actionnés par le requérant, ne signifie pas pour autant que l'article 8 de la Convention se trouve *ipso facto* respecté. Le raisonnement de la Cour de cassation française qui a refusé de reconnaître l'intérêt à agir d'une personne, sous prétexte que ses conversations avaient été écoutées sur la ligne d'un tiers, « pourrait conduire à des décisions privant de la protection de la loi un nombre très important de personnes » et « reviendrait, en pratique, à vider le mécanisme protecteur d'une large partie de sa substance » ; il y avait dès lors contrariété avec l'article 8 (268).

L'absence de garanties procédurales, claires, accessibles et effectives réglant les écoutes auxquelles il est procédé dans le cadre du programme Echelon est dès lors de nature à entraîner la violation de l'article 8 de la Convention européenne des droits de l'homme. Que ce soit au stade de l'examen de la légalité de l'ingérence ou à celui de sa nécessité dans une société démocratique, le contrôle du respect des droits processuels qu'il garantit n'étant qu'une nouvelle facette dudit contrôle de nécessité. Droits processuels minimaux dont certains sont également portés par l'article 13 de la Convention.

2. Le droit à un recours effectif pour contester Echelon devant une instance nationale et l'article 13 de la Convention

46. La seconde disposition de la Convention au regard de laquelle Echelon est critiquable est son article 13 qui garantit à la personne qui se plaint d'une violation de la Convention le droit à un recours effectif devant une

(264) Arrêt *Klass*, § 58.

(265) La décision *Christie contre Royaume Uni* (*supra*) semble avoir fait preuve de beaucoup de mansuétude sur cette garantie de la notification puisque si le requérant n'avait eu vent par des indiscrétions des interceptions de téléfax, il n'aurait sans doute jamais envisagé de saisir les autorités britanniques de contrôle.

(266) Voyez *supra* et en particulier les §§ 33 à 35 de l'arrêt *Huvig c. France* du 24 avril 1990 ainsi que l'arrêt *Valenzuela Contreras c. Espagne* du 30 juillet 1998.

(267) Chapitre III de la Directive 95/46/CE et article 14.2 de la Directive 97/66/CE, toutes deux précitées.

(268) Arrêt *Lambert c. France* du 24 août 1998, § 38.

instance nationale. Plusieurs arrêts ont condamné des Etats dont le droit ne prévoyait pas de recours du tout ou des recours insuffisamment effectifs pour contester des écoutes téléphoniques ou des fichages par les services de renseignement (I.B.2.a.).

Mais l'article 13 présente également l'avantage de faire l'objet d'une jurisprudence récente qui en accroît considérablement la portée. En en faisant pour les Etats parties à la Convention le siège d'obligations de prévention d'événements donnés ou d'enquête et de répression vis-à-vis des auteurs de ceux-ci, la Cour européenne des droits de l'homme complète l'éventail d'obligations positives que les autres dispositions de la Convention comportent. Cette autre évolution jurisprudentielle qui met à jour des obligations de vigilance (bien connues en droit des gens) permet de contester désormais avec moins de difficultés les violations structurelles de la Convention (I.B.2.b.). Or Echelon présente toutes les caractéristiques d'un système structurel de violations de celle-ci, sachant que toute interception de type téléphonique constitue à chaque fois une ingérence dans la vie privée, chaque ingérence devant être individuellement justifiée au regard de la Convention.

a) *L'analyse classique de l'article 13 : des recours nationaux insuffisants pour contester Echelon*

47. Les reproches visant Echelon et tenant à l'absence de garanties procédurales développés à propos de l'article 8 se répercutent également dans le droit à un recours effectif — Le droit garanti par l'article 13 de la Convention consiste à voir une instance statuer sur la violation alléguée de la Convention et à obtenir, s'il y a lieu, réparation (269). Cette disposition « présente d'étroites affinités » avec l'article 35, § 1^{er}, de la Convention qui pose parmi les conditions de recevabilité de n'importe quelle requête que celui, Etat ou particulier, qui la présente doit avoir au préalable épuisé les voies de recours internes (270). Pour pouvoir saisir une instance nationale d'un recours contestant une violation de la Convention, le requérant doit au moins faire valoir un grief « défendable » (271).

La Cour, dans l'affaire *Klass*, n'avait pas conclu à la violation de l'article 13 et ce, pour les mêmes motifs que ceux exposés à propos de l'article 8. Il a toutefois été posé que l'absence de violation de l'article 8 ne

(269) Notamment l'arrêt *Leander contre Suède* du 26 mars 1987, § 77.

(270) Arrêt *Aksoy c. Turquie* du 18 décembre 1996, § 51. Et *infra* quant à l'épuisement des voies de recours internes.

(271) Arrêt *Powell et Rayner c. Royaume Uni* du 21 février 1990, §§ 31-33. On peut s'attendre à ce que les pays participant activement ou passivement à Echelon soulèvent ce genre d'exception. C'est là tout l'intérêt attendu du rapport de la commission temporaire du Parlement européen même si tous les éléments présentés dans la partie I.A. paraissent désormais suffisants, au moins pour établir l'existence d'un réseau d'écoute à l'échelle mondiale.

signifiait pas *ipso facto* que l'article 13 serait respecté. Le droit à un recours effectif a déjà été jugé violé dans une affaire d'interrogatoire consécutif à une manifestation sur la voie publique car la Cour constitutionnelle autrichienne n'accueillait que les recours arguant de l'emploi de la force par la police, à l'exclusion de ceux qui reprochaient seulement l'établissement d'une fiche qui n'avait pas nécessité la contrainte physique (272).

L'article 13 doit donc pouvoir être invoqué même si la Cour ne constate pas de violation de l'article 8, sinon nul ne serait à même d'établir une violation de la Convention devant une instance nationale s'il ne pouvait saisir une telle instance. L'instance nationale peut ne pas être judiciaire mais l'examen du respect de l'article 13 nécessite alors un contrôle approfondi des pouvoirs et garanties procédurales offerts dans chaque cas (273). Il importe de rappeler que, dans l'affaire *Klass*, plusieurs recours étaient offerts à partir de la notification de ce qu'une interception avait eu lieu (274).

Il arrive certes que, alors qu'un constat de violation de l'article 8 a été établi par ailleurs, la Cour n'estime pas utile de se prononcer sur l'éventuelle violation de l'article 13 (275).

Mais on dénombre plusieurs arrêts récents qui ont conclu tant la violation de l'article 8 qu'à celle de l'article 13.

L'arrêt *Halford contre Royaume Uni* a estimé l'article 13 violé dans la foulée de l'article 8 puisque, pas plus que n'étaient réglementées par le droit anglais les écoutes auxquelles il avait été procédé sur le téléphone professionnel d'un officier de police, n'existait une quelconque mesure permettant d'obtenir le redressement de ce grief devant une instance nationale (276).

Deux arrêts datant de 2000 ont également établi la double violation des articles 8 et 13. L'arrêt *Rotaru contre Roumanie* tout d'abord, dans lequel il est apparu que la législation roumaine ne permettait de contester ni la conservation de données par les services de renseignement, ni leur véracité. Même si, au sens de l'article 13, les voies de recours ne doivent pas nécessairement être judiciaires et ne peuvent, en cas de surveillance secrète, s'ouvrir qu'une fois la mesure divulguée, il faut qu'existe absolument un recours effectif qui faisait défaut en l'espèce (277).

(272) Même si l'affaire s'est clôturée par un règlement amiable qui a entraîné sa radiation du rôle de la Cour (arrêt du 31 janvier 1995), le rapport précité de la Commission du 19 mai 1994, req. n° 15225/89, *Freidl c. Autriche*, § 77, a bel et bien établi que la consignation de données personnelles consécutivement à des prises de vue par la police lors d'une manifestation ne violait pas l'article 8 mais violait l'article 13 en l'absence de recours effectif.

(273) Arrêt *Klass c. Allemagne* du 4 juillet 1978, § 67.

(274) La Cour n'a pas estimé non plus l'article 13 violé dans son arrêt *Amann c. Suisse* dans la mesure où les recours existaient et avaient bel et bien été actionnés (§ 89).

(275) Arrêt *Malone c. Royaume Uni* du 27 juin 1984, 90.

(276) Arrêt *Halford c. Royaume Uni* du 25 juin 1997, § 65.

(277) Arrêt *Rotaru c. Roumanie* du 4 mai 2000, §§ 69-71.

Quant à l'arrêt *Khan contre Royaume Uni*, il a aussi conclu à la violation de l'article 13 après celle de l'article 8 aux motifs que les plaintes pour contester une écoute devant la *Police Complaint Authority* ne pouvaient concerner que les cas de meurtres ou de sérieux dommages corporels et les cas indiqués par le Secrétaire d'Etat, d'une part, et surtout que ladite autorité n'était pas suffisamment indépendante du Secrétaire d'Etat (qui en appointait et pouvait en révoquer les membres) dont elle devait suivre les instructions (278).

L'article 13 de la Convention requiert dès lors des obligations relativement précises, en particulier l'existence d'un organe de recours indépendant de celui qui a procédé ou fait procéder à une interception. Une autre obligation, également prévue par l'article 8, § 2, de la Convention dans le cadre du contrôle de nécessité, résulte de l'imposition de principe de la notification de l'interception, de l'écoute ou de la conservation de données personnelles :

« The duty to notify is a principle that can be put aside if the data are deleted shortly after their collection or if the notification would imply a disproportionate effort. But in principle there is a duty to notify. This is the result of the acknowledgment of the legally relevant tie between a person and the data held by others. The person must be enabled to exercise his rights with regard to his data. Article 13 of the Convention on Human Rights guarantees an effective remedy against any intrusion of rights that the Convention grants. A remedy cannot be effective if a person does not know about the processing of his data » (279).

Les arguments développés ailleurs sur l'absence de garanties procédurales (contrôles de « légalité » et de « nécessité » dans le cadre de l'article 8) et de recours à épuiser valablement à l'encontre du programme Echelon (II.B.1.) peuvent donc venir étayer l'éventuelle contrariété de celui-ci avec l'article 13 de la Convention, en particulier en ce qui concerne l'exigence de l'indépendance des organes de contrôle des écoutes téléphoniques et, plus simplement, parce que l'on voit mal en quoi, par exemple, une italienne téléphonant d'Italie en France devrait s'adresser à des organes de contrôle allemand ou anglais parce que la NSA et les services tiers collaborant avec elle intercepte ses conversations à partir des sols allemand ou anglais.

b) *L'analyse nouvelle de la place de l'article 13 dans l'ensemble de la Convention : Echelon, un cas de violation structurelle et de manquement à une obligation de vigilance*

48. Il existe un devoir de réaction existant en cas de violation grave des droits de l'homme sur le territoire d'un Etat — Le Comité

(278) Arrêt *Khan c. Royaume Uni* du 12 mai 2000, §§ 45-47.

(279) A. PATIJN, *op. cit.*, p. 19. Les cas où la notification n'est pas requise étant des exceptions au principe sont d'interprétation restrictive. En ce qui concerne celui où notifier requerrait un effort disproportionné, on imagine mal, si une interception intervient dans une structure systématique comme Echelon que le caractère imposant d'une telle structure soit justement le motif justifiant l'absence de notification, sans quoi cela reviendrait à donner aux États un chèque en blanc pour créer des banques de données toujours plus imposantes.

des Droits de l'homme de l'O.N.U. estime que les procédures de caractère administratif ne sauraient être considérées comme des recours utiles et suffisants au sens de l'article 2 du Pacte international relatif aux droits civils et politiques en cas de violation particulièrement grave des droits de l'homme (280). En adhérant au Pacte,

« l'Etat partie est tenu de protéger effectivement les droits des auteurs et de veiller à ce que des violations analogues ne se reproduisent à l'avenir » (281).

La Cour européenne va dans le même sens à propos des violations graves comme celles de l'article 3 de la Convention qui prohibe la torture. Pour peu que le grief soit suffisamment défendable, l'article 13 requiert une enquête approfondie et effective ainsi que l'accès du requérant à l'enquête, la poursuite et la punition des coupables et, s'il échet, une réparation (282).

Lorsqu'est en cause un droit aussi éminent que celui à l'intégrité physique (article 3 de la Convention), un Etat peut certes invoquer l'absence d'épuisement des voies de recours internes (283) mais verra son exception préliminaire rejetée, même dans le cas où il aurait procédé à une enquête, si celle-ci n'était pas suffisamment effective (284). Pour que soit effectif le recours, son exercice ne doit pas être entravé de manière injustifiée par les actes et omissions de l'Etat défendeur (285).

(280) C.D.H., décision du 29 juillet 1997, com. n° 612/1995, *Vicente et autres c. Colombie*, point 8.2. La Cour européenne semble aller moins loin en ce qui concerne les enquêtes de sécurité dans la fonction publique puisque malgré le constat des faiblesses présentées par les modes suédois de contrôle, elle a néanmoins affirmé que pris dans leur ensemble ces moyens, même non judiciaires, étaient suffisants dans les circonstances de l'affaire *Leander* (§ 84). L'opinion partiellement dissidente du juge RYSDALL estimait d'ailleurs le contraire. Quant à l'opinion partiellement dissidente des juges PETITTI et RUSSO, elle relevait à juste titre que des recours inefficaces, même additionnés, ne peuvent constituer un recours effectif et que l'Etat ne peut être totalement juge et partie en matière de surveillance secrète.

(281) C.D.H., décision du 29 juillet 1997, com. n° 549/1993, *Hopu et Bessert c. France*, point 12. Le C.D.H. estime notamment que « l'Etat partie a le devoir de mener des enquêtes approfondies sur les violations supposées des droits de l'homme en particulier lorsqu'il s'agit de disparitions forcées et d'atteintes au droit à la vie, et d'engager des poursuites pénales contre quiconque est présumé responsable de ces violations, de procéder au jugement et de prononcer une peine » (décision du 29 juillet 1997, com. n° 612/1995, point 8.8, souligné par nous).

(282) Le millésime 1998 fut particulièrement fructueux sur la portée effective de l'article 13 de la Convention, comme en attestent les arrêts recensés par P. LAMBERT, « La Cour européenne des droits de l'homme — année 1998 », *J.T.D.E.* 1999, pp. 39-40. Egalement, entre autres, l'arrêt *Ihlan c. Turquie* du 27 juin 2000, § 97.

(283) Le principe de l'épuisement des voies de recours internes porté par l'article 35 de la Convention est une règle de procédure intimement liée à la règle de fond portée par l'article 13. C'est pourquoi le raisonnement peut être étendu ici au droit à un recours effectif.

(284) Notamment dans l'arrêt *Selmouni c. France* du 28 juillet 1999, § 79, la Cour dit qu'« il s'agit moins de savoir s'il y a eu une enquête, puisque son existence est avérée, que d'apprécier la diligence avec laquelle elle a été menée, la volonté des autorités d'aboutir à l'identification des responsables ainsi qu'à leur poursuite et, partant, son caractère 'effectif'. Cette question revêt un aspect particulier si l'on se rappelle que, lorsqu'un individu formule une allégation défendable de violation des dispositions de l'article 3 (ainsi que d'ailleurs de l'article 2), la notion de recours effectif implique, de la part de l'Etat, des investigations approfondies et effectives propres à conduire à l'identification et à la punition des coupables ».

(285) Arrêt *Salman c. Turquie* du 27 juin 2000, § 121.

La Cour interaméricaine des droits de l'homme ne s'est pas exprimée autrement dans son désormais célèbre arrêt *Velasquez* quand, en se penchant sur les cas de « disparitions », elle a mis, de manière générale, à charge des Etats une « obligation de diligence » à l'égard des actes se déroulant sur leur territoire :

« Il est clair qu'en principe est imputable à l'Etat toute violation des droits reconnus par la Convention [interaméricaine des droits de l'homme] résultant d'un acte des pouvoirs qu'ils tirent de leurs fonctions officielles. Cela n'épuise cependant pas les situations où un Etat est obligé de prévenir, rechercher et sanctionner les violations des droits de l'homme, ni les cas où sa responsabilité peut se voir engagée pour atteinte à ces mêmes droits. En effet, un acte attentatoire aux droits de l'homme et qui, initialement, ne serait pas directement imputable à un Etat — par exemple s'il est l'œuvre d'un particulier ou si son auteur n'est pas identifié — peut néanmoins engager la responsabilité internationale de cet Etat, non en raison du fait lui-même, mais en raison du manque de diligence de l'Etat pour prévenir la violation des droits de l'homme ou la traiter dans les termes requis par la Convention » (286).

49. Les obligations de réaction portées par l'article 13 de la Convention concernant également Echelon — Il existe donc en matière de droits de l'homme une « obligation de diligence due » ou « obligation de vigilance » qui impose tant des devoirs préventifs, pour en empêcher la violation, que répressifs, afin de poursuivre et punir effectivement les auteurs de l'atteinte aux droits garantis (287). A un moment où la doctrine la plus récente constate unanimement le regain d'intérêt de la Cour pour l'article 13 de la Convention (droit à un recours effectif), cela a d'autant plus d'importance.

Ces obligations ont été fréquemment rappelées dans des affaires turques, à tel point que Jean-François Flauss peut voir dans l'actuelle jurisprudence de la Cour un renforcement des standards de protection favorable aux victimes de violations structurelles (288). Or, le risque effectif de violation structurelle et systématique du droit au respect de la vie privée que peut représenter Echelon paraît également commander une telle lecture de l'article 13 de la Convention, sans préjudice de l'obligation classique de vigilance que le droit international impose à l'Etat sur son territoire (289). Les griefs pesant sur les Etats pouvant participer à Echelon ne concernent certes pas les droits indérogeables comme ceux garantis par les articles 2 et 3 de la Convention. Néanmoins, la gravité des violations de la Convention résultent de leur caractère manifeste (notamment en raison de l'absence avérée d'accessibilité des règles juridiques censées présider à son fonctionne-

(286) Cour interam.d.h., arrêt *Velasquez c. Honduras* du 29 juillet 1988, § 172, extraits in. *R.G.D.I.P.* 1990, p. 467, précédé des commentaires de G. COHEN-JONATHAN. Souligné par nous.

(287) P. APRAXINE, « Violation des droits de l'homme par une organisation internationale et responsabilité des Etats au regard de la Convention européenne », *R.T.D.H.* 1995, p. 27.

(288) J.F. FLAUSS, « La Cour de Strasbourg face aux violations systématiques des droits de l'homme », in *Mélanges P. Lambert*, Bruxelles, Bruylant, 2000, pp. 348-353.

(289) *Infra*.

ment) et structurel (notamment en raison du caractère exploratoire et général qui est prêté à Echelon et du caractère secret qui l'entoure).

De surcroît, l'article 13 n'établit aucune distinction selon que l'acte dont il est allégué qu'il viole la Convention émane du pouvoir judiciaire, du pouvoir législatif ou du pouvoir exécutif. Dans ce dernier cas, il interdit d'ailleurs qu'un Etat se prévale de l'exception selon laquelle les « actes de gouvernement » ne seraient pas justiciables de la Convention (290), de telle sorte que même les domaines « régaliens » du maintien de l'ordre, de la défense et des relations extérieures ne font pas échapper l'Etat à ses obligations de vigilance et à la responsabilité internationale qui s'ensuit lorsqu'il y manque (291).

Dès lors, l'article 13 de la Convention saurait d'autant moins faire obstacle à l'imputabilité aux Etats parties, qu'ils participent de près ou de loin à Echelon, que les devoirs positifs de réaction consécutifs au respect du droit à un recours effectif sont de plus en plus nombreux à être dégagés par la Cour européenne des droits de l'homme.

2^e Partie. — LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME
EST UN INSTRUMENT EFFICACE POUR CONTRER LES ETATS PARTIES
QUI PARTICIPENT À ECHELON

50. Si la première partie s'attache à l'établissement des faits et à la description de certaines des obligations internationales que les Etats participant à Echelon violeraient, la seconde partie doit analyser comment la responsabilité internationale de ces Etats peut être mise en œuvre. Il faut d'abord montrer que cette participation est imputable à des Etats parties à la Convention, qu'ils agissent ou non avec des Etats tiers non parties étant à cet égard indifférent (II.A.). Le caractère secret, global et international d'Echelon n'est pas plus un obstacle à la recevabilité des recours étatiques ou individuels qui seraient introduits devant la Cour européenne des droits de l'homme (II.B.).

(290) D. DE BRUYN, « Le droit à un recours effectif », in *Mélanges P. Lambert*, Bruxelles, Bruylant, 2000, pp. 188-189.

(291) R. ERGEC, « Le contrôle juridictionnel de l'administration dans les matières qui se rattachent aux rapports internationaux : actes de gouvernement ou réserve de pouvoir discrétionnaire? », *R.D.I.D.C.* 1986, p. 131. L'invocation de l'« acte de gouvernement » ne peut donc emporter l'incompétence des juridictions nationales ou internationales à l'égard des Etats parties; elles sont au contraire compétentes pour statuer sur les questions de fond et d'imputabilité posées. On notera au passage ici que la réserve de la sécurité nationale a bel et bien été intégrée dans la Convention, notamment dans son article 8, § 2; elle ne peut être invoquée au plan procédural mais peut l'être seulement au fond. C'est alors, pour peu qu'aient été préalablement respectées les exigences de légalité et de légitimité, qu'intervient, lors de l'examen de la nécessité des ingérences, le contrôle de leur proportionnalité avec l'objectif de protection de la sécurité nationale.

A. — *L'imputabilité de la violation des obligations internationales
portées par la Convention européenne des droits de l'homme —
Réseau international de surveillance électronique
et « juridiction » des Etats parties*

51. Des questions spécifiques relatives à l'imputabilité peuvent être soulevées dans le cadre du programme Echelon puisqu'il semble être déployé par plusieurs Etats et sortir ses effets bien au-delà du territoire de ceux-ci. De surcroît, certains Etats sont Parties à la Convention, soit l'Allemagne et le Royaume Uni (292), alors que d'autres ne le sont pas, soit l'Australie, la Canada, les Etats Unis, le Japon et la Nouvelle Zélande. Cette circonstance n'exonère cependant en rien les Etats Parties à la Convention de leur responsabilité à l'égard de celle-ci.

Le problème de l'imputabilité des actes querellés aux Parties à la Convention se situe aux confins des questions de procédure (établissement de la compétence de la Cour à l'égard des seuls Etats Parties) et de fond (établissement de la responsabilité proprement dite pour violation d'obligations internationales). En y adhérant, les Etats n'ont nullement dérogé aux règles traditionnelles d'imputabilité (II.A.1). En procédant à l'imputabilité à des Etats parties de faits apparemment complexes en ce qu'ils naissent des relations nouées avec d'autres Etats, même non parties, la Cour a contribué à considérablement renforcé la portée des obligations souscrites lors de l'adhésion à la Convention (II.A.2).

1. *Echelon et les règles classiques de la responsabilité internationale*

52. Deux types de comportements peuvent faire l'objet de critiques au regard de la Convention et être imputés à des Etats parties en vertu des règles traditionnelles de la responsabilité internationale. Il s'agit de comportements étatiques « actifs », c'est-à-dire lorsqu'un Etat procède lui-même à des écoutes et interceptions : la violation de la Convention est alors « directe ». Elle découle d'une action imputable à l'Etat par application de la théorie classique de l'organe (II.A.1.a).

(292) Les cas d'autres pays signataires de la Convention européenne des droits de l'homme, qu'ils soient membres ou non de l'Union européenne, pourraient également être abordés. Mais les sources sur leur implication exacte dans Echelon sont moins nombreuses que celles établissant que l'Allemagne accueille au moins une base de la NSA à Bad Aibling (cartes citées en introduction concordantes, rapport « Campbell »,...) et que le Royaume Uni, non content de cogérer avec la NSA au moins la base de Menwith Hill, la plus importante base du monde, est partie fondatrice à l'accord UKUSA (sources officielles anglaises et américaines) et, comme cela a été établi par l'ancienne Commission européenne des droits de l'homme dans l'affaire *Christie*, procède au moins, à l'aide du « Dictionary », à l'interception de tout ce qui entre et sort de Londres. Néanmoins, comme il est possible que d'autres Etats accueillent des bases sur leur territoire, le raisonnement ici tenu à propos des obligations de vigilance sur leur territoire est intégralement applicable.

Mais il s'agit également de critiquer des comportements étatiques « passifs », c'est-à-dire lorsqu'un État laisse un corps quelconque, privé ou public, ressortissant d'un État Partie ou non, commettre des faits en contrariété avec le droit au respect de la vie privée sans pour autant participer aux écoutes; l'État est également responsable de ses omissions et de ses violations « indirectes » du droit international qui en découlent (II.A.1.b).

a) *En vertu de la théorie de l'organe, un État est responsable des agissements de ses services secrets : la participation « active » à Echelon*

53. Un principe simple — Au terme de l'article 3 du projet de la Commission du Droit International de l'ONU sur la responsabilité internationale des États,

« il y a fait internationalement illicite de l'État lorsque : a) un comportement consistant en une action ou une omission est attribuable, d'après le droit international, à l'État; et b) que ce comportement constitue une violation d'une obligation internationale » (293).

Les États sont responsables du comportement de leurs organes (article 5), quelle que soit la position de l'organe dans l'organisation de l'État (article 6), que l'organe soit celui d'une collectivité territoriale ou de toute entité habilitée par le droit interne à exercer des prérogatives de la puissance publique (article 7).

Peuvent également être attribués à l'État le comportement de personnes agissant en fait pour son compte (article 8), celui d'organes mis à sa disposition par un autre État ou une organisation internationale (article 9) et, dans tous ces cas, le comportement d'organes outrepassant leurs compétences ou contredisant leurs instructions (article 10).

Toutes ces hypothèses n'appellent pas de commentaires particuliers puisqu'il s'agit de tirer les conséquences qui s'attachent au principe classique

(293) Le texte est celui du projet d'articles adopté en 1996 à titre provisoire par la C.D.I. qui vise à codifier le droit international applicable à la responsabilité internationale des États (Rapport de la C.D.I. sur les travaux de sa 48^e session, Doc.off. A.G., 51^e session, supp. n° 10 (A/51/10), pp. 148 et s.). Il n'a pas été possible de dûment tenir compte de ce que le comité de rédaction de la Commission de droit international a provisoirement adopté le 11 août 2000 lors de sa 52^e session une nouvelle mouture du projet sur la responsabilité internationale des États (A/CN.4/L.600) qui préserve la rédaction des articles 5 à 10 (sauf l'article 6 sur l'indifférence de la position hiérarchique de l'organe dans la mesure où elle va de soi et en proposant un nouvel article 8bis sur l'attribution à l'État d'un certain comportement mené en l'absence des autorités officielles). Ceux-ci sont renumérotés sans changer fondamentalement. Il est proposé de supprimer les articles 11 à 14 dont le principe commun est cependant repris dans une proposition unique de nouvel article 11 (un comportement non attribuable à l'État en vertu des articles 5 et suivants est néanmoins considéré comme un fait de cet État si et dans la mesure où l'État entérine et fait sien le comportement en question). Les parties portant sur la responsabilité des organisations internationales ou pour le comportement de celles-ci ont été retirées du projet adopté provisoirement cette année. Ce sont donc les articles dans l'état de leur rédaction en 1996 qui figurent ici, sachant qu'il a été évidemment tenu compte des rapports rédigés par le prof. CRAWFORD de l'Université de Cambridge qui ont guidé les travaux de la C.D.I.

de l'unité de l'Etat en droit international. Si l'Etat peut être tenu pour responsable des actions et omissions de n'importe laquelle de ses autorités, les activités de ses services secrets engagent donc la responsabilité internationale d'un Etat (294), que ces activités se déploient sur son territoire ou en dehors de celui-ci.

L'Etat peut donc engager sa responsabilité internationale en raison du fait direct de ses organes ou de personnes agissant pour son compte conformément aux articles 5 à 10 du projet de la C.D.I. L'article 5 (théorie élémentaire de l'organe) permet plus particulièrement de rencontrer l'hypothèse où un Etat partie à Echelon procède par lui-même à des interceptions de télécommunications, comme c'est le cas du Royaume Uni en exécution de l'accord UKUSA dont il est partie fondatrice, que ses services de renseignement agissent à partir du territoire britannique, sur un territoire tiers avec l'accord de l'Etat hôte ou sans l'accord de l'Etat sur le territoire duquel elles ont lieu. Les interceptions extra-frontalières violent, comme cela a été longuement vu plus haut, le principe de territorialité à la base du droit des gens, et les strictes conditions de leur validité au regard de l'article 8 de la Convention européenne des droits de l'homme.

b) *Lorsqu'un Etat est titulaire d'une obligation spécifique, il encourt une responsabilité propre en raison des agissements d'une puissance tierce sur son territoire : la participation « passive » à Echelon*

54. Un Etat n'est en principe pas responsable de tous les événements se déroulant sur son territoire — Le critère le plus fréquent pour l'exercice des compétences de l'Etat en droit international reste avant toute chose le critère territorial; il en va de même dans le cadre de la Convention. Le territoire national est en effet le premier titre de « juridiction » des Etats. La souveraineté territoriale emporte la plénitude de son propre contenu et l'exclusivité de son exercice. La souveraineté s'exerce donc à l'égard de toutes les personnes se trouvant sur le territoire; même la compétence personnelle à l'égard des nationaux situés en territoire étranger est, en principe, limitée par la compétence territoriale de l'Etat hôte.

Certes, comme l'a souligné la Cour Internationale de Justice, un Etat ne peut systématiquement être tenu pour responsable, au regard du droit international général, de tous les actes qui se déploient sur son territoire (295). Il est de surcroît admis que

« une fois qu'un Etat a consenti à l'établissement, sur son territoire, de services publics étrangers, il perd tout droit de regard sur leur fonctionnement, qui relève de la compétence exclusive de l'Etat bénéficiaire » (296).

(294) J. SALMON et E. DAVID, *Droit des gens*, t. IV, 15^e éd., Presses Universitaires de Bruxelles, 1999-2000, p. 650.

(295) C.I.J., *Affaire du Détroit de Corfou*, Rec. 1949, p. 4, p. 18.

(296) N. QUOC DINH, P. DAILLIER et A. PELLET, *Droit International Public*, op. cit., p. 499.

55. Ce principe n'empêche cependant pas qu'un Etat reste tenu de ses actions et omissions propres en rapport avec les événements se déroulant sur son territoire — Si l'article 12 du projet de la C.D.I. dispose bien que n'est pas considéré comme fait de l'Etat le comportement adopté sur son territoire par l'organe d'un autre Etat agissant en cette qualité, il comporte toutefois un paragraphe 2 qui préserve l'imputabilité au premier Etat des comportements de ses propres organes ou des personnes qui agissent pour son compte (soit les cas réglés par les articles 5 à 10 précités), s'ils ont manqué aux obligations, en relation avec les agissements de l'Etat tiers, qui leur incomberaient par ailleurs en propre.

Il en va de même en ce qui concerne les activités d'une organisation internationale. L'article 13 du projet de la C.D.I. sur la responsabilité internationale des Etats dispose que ne peut être imputé à un Etat le comportement d'une organisation internationale du seul fait que ledit comportement aurait été adopté sur son territoire. Il est vrai que cet article 13 ne comporte pas explicitement de clause qui réserve le cas où l'Etat pourrait se voir imputer un manquement découlant du comportement de ses organes ou des personnes qui agissent pour son compte. Cette absence ne saurait cependant empêcher la responsabilité propre de l'Etat hôte s'il omet de réagir de façon appropriée à l'accomplissement d'actes illicites par les organes d'une organisation internationale (297).

Donc, l'Etat, même s'il ne peut être tenu *a priori* des agissements sur son territoire de tierces personnes privées (article 11, § 1^{er}, du projet de la C.D.I.) ou internationales, c'est-à-dire du fait des organes d'un autre Etat (article 12, § 1^{er}) ou d'une organisation internationale (article 13), n'engage cependant pas moins sa responsabilité internationale si le comportement de ses organes (conformément aux articles 5 à 10) est en rapport avec le fait de personnes privées (article 11, § 2), d'un Etat tiers (article 12, § 2) ou d'une organisation internationale (même si l'article 13 ne le prévoit pas). Ce qui ne revient jamais qu'à appliquer la théorie de l'organe dans une situation particulière.

De manière générale, le droit des gens prescrit en effet que

« sous peine d'abus de droit, [l'Etat] doit faire usage de ses pouvoirs dans l'intérêt général de la population, sans nuire à la communauté internationale, et plus particulièrement aux Etats voisins » (298).

Autrement formulée par la Cour internationale de justice, il existe une

« obligation pour tout Etat de ne pas utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats » (299).

(297) P. APRAXINE, « Violation des droits de l'homme par une organisation internationale et responsabilité des Etats au regard de la Convention européenne », *R.T.D.H.* 1995, p. 25.

(298) N. QUOC DINH, P. DAILLIER, A. PELLET, *Droit international public*, 6^e éd., Paris, LGDJ, 1999, p. 471.

(299) C.I.J., *Affaire du Détroit de Corfou*, précitée, p. 22; également le projet de résolution élaboré en janvier 1999 au sein de l'Institut de Droit International, précité. L'hypothèse de la com-

La responsabilité internationale peut ainsi découler de la négligence propre de l'Etat qui manque à ses devoirs propres quant à l'usage de son territoire. La pratique internationale montre que, s'il ne peut être tenu du comportement de personnalités internationales tierces, en ce compris des services de renseignement étrangers, par cela seul que leurs agissements ont lieu sur son territoire,

« l'Etat territorial doit cependant demeurer vigilant à propos de ce qui se passe sur son territoire » (300).

Sur cette base, les Etats qui, à l'instar de l'Allemagne, accueillent des stations Echelon engagent leur responsabilité parce que leurs organes ne réagissent pas de manière appropriée à la mise à disposition de leur territoire pour la commission, par les organes d'Etats tiers, d'actes internationalement illicites que sont au regard du droit international général les écoutes téléphoniques extra-territoriales, d'une part, actes posés en violation des conditions de validité des interceptions telles que portées par la Convention européenne des droits de l'homme, d'autre part. Or la Convention porte des obligations de vigilance d'une nature particulière fondées, notamment, sur son article 13.

2. Les conséquences de l'adhésion à la Convention pour la responsabilité internationale des Etats participants à Echelon

a) *Un Etat participant à Echelon ne peut méconnaître la nature particulière des obligations souscrites dans la Convention*

56. La Convention ne s'écarte pas des règles classiques d'imputabilité mais met à charge des Etats des obligations particulièrement

plicité n'est pas non plus à exclure dans les cas où un Etat fournit à un autre Etat son territoire pour établir des bases pour les services secrets de celui-ci en vue de commettre des faits illicites (J. SALMON et P. KLEIN, *op. cit.*, p. 132). Elle n'est cependant pas retenue ici dans la mesure où, si l'Allemagne et le Royaume Uni abritent des stations d'écoute américaines, les Etats Unis ne sont pas Parties à la Convention et ne peuvent donc attrait devant la Cour de Strasbourg. Sur l'implication d'un autre Etat dans la commission d'un fait internationalement illicite par un autre Etat : J. CRAWFORD, *Deuxième rapport sur la responsabilité internationale des Etats*, 51^e session de la C.D.I., A/CN.4/498/Add.1, pp. 2-6. De surcroît, pour que puissent jouer les règles telles que codifiées par la C.D.I., il faut en principe, à moins que les Etats concernés n'aient adopté une *lex specialis*, que l'Etat A qui « aide » un Etat B à la commission d'un fait internationalement illicite soit également tenu par les obligations qui sont celles de l'Etat B vis-à-vis de l'Etat C dont les ressortissants ou lui-même subissent le préjudice (J. CRAWFORD, *Third report on State responsibility*, distribué le 1^{er} juillet 2000, 52^e session de la C.D.I., A/CN.4/507/Add.2). Une telle hypothèse ne se rencontre pas, vis-à-vis des Etats Unis dans le cadre de la mise en œuvre de la Convention, puisque les Etats Unis n'y sont pas parties, pas plus que dans le cadre du Pacte International relatif aux droits civils et politiques. Du moins si l'on a égard au mécanisme de la communication individuelle auquel ils n'ont pas souscrit. Car, ayant par contre reconnu la compétence du Comité des droits de l'homme à l'égard des communications étatiques, la complicité pourrait être invoquée à leur encontre (II.B.3).

(300) J. SALMON et P. KLEIN, *Responsabilité internationale*, t. I, Presses Universitaires de Bruxelles, 1998-1999, p. 96 ainsi que les pp. 83-92 pour les cas de responsabilité pour comportement de particuliers.

fortes — Le degré d'intégration de la Convention dans les droits internes des Etats Parties ne saurait faire oublier qu'elle constitue avant tout une norme de droit international dont la violation emporte la responsabilité internationale des Parties (301). Pour pouvoir invoquer une violation de la Convention européenne des droits de l'homme, il faut donc établir que ladite violation est imputable à un Etat Partie. Il faut ainsi démontrer que celui-ci a exercé sa « juridiction » au sens de l'article 1^{er} qui stipule que

« les Hautes Parties contractantes reconnaissent à toute personne relevant de leur juridiction les droits et libertés définis au titre I de la présente Convention » (302).

Il a été vu plus haut, à propos de son article 13, que les obligations contractées par les Etats en adhérant à la Convention européenne des droits de l'homme ne consistent pas seulement dans le devoir de s'abstenir de la violer : ils sont aussi débiteurs d'« obligations positives » (303). Les Etats, disposant pour ce faire d'une certaine marge d'appréciation, sont en effet tenus d'adopter certaines mesures aptes à assurer le respect effectif et concret des droits garantis par la Convention (304).

La théorie des obligations positives voit dans l'applicabilité potentielle des droits fondamentaux dans les rapports entre particuliers son terrain de prédilection : il s'agit ici de la reconnaissance de l'applicabilité horizontale des droits de l'homme ou « *Drittwirkung* », désormais bien ancrée dans le corpus jurisprudentiel strasbourgeois (305). La Cour européenne des droits de l'homme aboutit de plus en plus souvent à condamner des Etats dans des affaires ayant leur origine dans des litiges entre particuliers pour manquement à l'obligation de veiller au respect des droits fondamentaux, y compris dans les relations entre particuliers : un tel manquement imputable à l'Etat engage sa responsabilité internationale (306).

(301) Cons. P. TAVERNIER, « La Cour européenne des droits de l'homme applique-t-elle le droit international ou un droit de type interne ? », in P. TAVERNIER (dir.), *Quelle Europe pour les droits de l'homme ?*, Bruxelles, Bruyant, 1996, pp. 17-37.

(302) Sur l'article 1^{er}, on consultera notamment J.A. CARRILLO-SALCEDO, « Article 1 », in. L.E. PETTITI, E. DECAUX et P.H. IMBERT (dir.), *La Convention européenne des droits de l'homme — Commentaire article par article*, 2^e éd., Paris, Economica, 1999, pp. 135-141 ; J.F. RENUCCI, *Droit européen des droits de l'homme*, Paris, L.G.D.J., 1999, pp. 343-345. Comme le pose l'arrêt *Irlande c. Royaume-Uni* du 18 janvier 1978, § 238, la violation de l'article 1^{er} en soi n'existe pas ; elle découle toujours de celle d'un autre article de la Convention.

(303) L'arrêt *Marckx c. Belgique* du 13 juin 1979, § 31, a été le premier à parler explicitement de l'existence d'obligations positives.

(304) Pour des exemples récents : l'arrêt *Stubbings et autres c. Royaume-Uni* du 22 octobre 1996, §§ 62-62 ; ou encore l'arrêt *Özgür Gündem c. Turquie* du 16 mars 2000, §§ 42-43. Voyez l'étude fondamentale de F. SUDRE, « Les 'obligations positives' dans la jurisprudence européenne des droits de l'homme », *R.T.D.H.* 1995, pp. 363-384. La Cour estime que les obligations positives et les obligations négatives ne se prêtent pas à une définition précise mais que les principes qui leur sont applicables sont comparables (arrêt *Ahmut c. Pays-Bas* du 28 novembre 1996, § 63).

(305) D. SPIELMANN, *L'effet potentiel de la Convention européenne des droits de l'homme entre personnes privées*, Bruxelles, Nemesis et Bruylant, 1995.

(306) Et ce même si certains parlent de responsabilité « indirecte » de l'Etat (E.A. ALKEMA, « The third-party applicability or 'Drittwirkung' of the European Convention on Human

L'article 11 du projet de la Commission du Droit International n'est, par conséquent, pas énérvé par la jurisprudence strasbourgeoise qui consolide la « drittwirkung ». En effet, la violation d'une obligation internationale par un particulier ne peut en principe être imputée à l'Etat (§ 1^{er}). Par contre celui-ci peut se voir imputer les actes de ses organes qui ont favorisé cette violation (§ 2). Or, le professeur Condorelli qui a étudié en détails les relations entre le projet de la CDI et la Convention européenne a très nettement établi que

« s'il y a orthodoxie, c'est que les règles primaires pertinentes [les obligations de fond à charge de l'Etat, les règles secondaires étant celles qui sanctionnent l'irrespect des premières] ne font peser sur les Etats, pour ce qui est des relations entre particuliers, rien de plus que des obligations de style classique (plus ou moins 'lourdes' au demeurant, suivant les cas) attendant à la 'diligence due'; il en découle pour lesdits Etats la nécessité de déployer tous les efforts possibles et raisonnables afin de prévenir et réprimer les atteintes aux droits de l'homme venant d'individus. Or, il est certain que rien ne saurait empêcher les Etats de souscrire à des obligations encore plus lourdes : ceux-ci pourraient par exemple accepter de considérer leur responsabilité engagée dès qu'une certaine violation des droits de l'homme se produit dans leur sphère de souveraineté, ou bien laisser jouer contre eux une présomption prima facie à cette intention » (307).

Il faut retenir de ces lignes que, d'une part, les Etats peuvent souscrire par une *lex specialis* (comme la Convention européenne des droits de l'homme) à des règles d'imputabilité plus contraignantes que celles portées par le projet de la C.D.I. (308). et que, d'autre part, les obligations de « vigilance » (aussi appelées de « diligence due ») occupent une place primordiale dans le droit des droits de l'homme (309).

L'hypothèse développée ici, parce qu'elle est la plus fréquente dans la jurisprudence strasbourgeoise, est celle de manquements à une obligation de vigilance propres à l'Etat et qui, bien que trouvant leur source dans le fait de personnes privées, lui restent cependant imputable. Un raisonnement identique doit être tenu à propos de l'Etat hôte dans le cas d'agissements sur son territoire d'Etats tiers ou d'organisations internationales en raison de l'obligation classique de vigilance portée par le droit international

Rights », in. *Mélanges G.J. Wiarda*, Karl Heymanns Verlag, Cologne, 1988, p. 42). L'arrêt *Artico c. Italie* du 13 mai 1980, § 36, n'a pas reproché à l'Etat italien la défaillance d'un avocat commis d'office mais bien sa passivité car il aurait dû remplacer l'avocat ou le pousser à s'acquitter de sa tâche.

(307) L. CONDORELLI, « L'imputation à l'Etat d'un fait internationalement illicite : solutions classiques et nouvelles tendances », *R.C.A.D.I.* 1984, VI, p. 154.

(308) Ce que confirme le *Premier rapport sur la responsabilité des Etats*, présenté par le rapporteur spécial J. CRAWFORD lors de la 50^e session de la C.D.I., A/CN.4/490/Add.5, p. 6.

(309) Sur les origines de l'obligation de vigilance à charge d'un Etat sur son territoire comme corollaire de sa souveraineté territoriale : P. REUTER, *Droit international public*, 6^e éd., Paris, P.U.F., 1983, pp. 256-259, qui parle de responsabilité pour négligence.

général. A plus forte raison si l'Etat hôte a adhéré à la Convention européenne des droits de l'homme (310).

57. Une obligation de vigilance renforcée dans le système européen parce que les Etats y ont contracté des obligations objectives — La nature même des obligations souscrites par les Etats parties à la Convention européenne des droits de l'homme rend cette exigence de vigilance particulièrement forte (311). Ces obligations sont objectives (312) ainsi que l'a affirmé ce passage célèbre de la décision de la Commission européenne des droits de l'homme dans l'affaire *Autriche contre Italie*,

« les obligations souscrites par les Etats Contractants dans la Convention ont essentiellement un caractère objectif, du fait qu'elles visent à protéger les droits fondamentaux des particuliers contre les empiètements des Etats Contractants, plutôt qu'à créer des droits subjectifs et réciproques entre ces derniers » (313).

L'arrêt *Irlande contre Royaume Uni* a complété le principe :

« A la différence des traités internationaux de type classique, la Convention déborde le cadre de la simple réciprocité entre Etats. En sus d'un réseau d'engagements synallagmatiques bilatéraux, elle crée des obligations objectives qui, aux termes de son Préambule, bénéficient d'une 'garantie collective'. (...) La Convention ne se contente pas d'astreindre les autorités suprêmes des Etats Contractants à respecter elles-mêmes les droits et libertés qu'elle consacre; (...) elle implique aussi qu'il leur faut, pour en assurer la jouissance, en empêcher ou corriger la violation aux niveaux inférieurs » (314).

L'ensemble qui réunit ces obligations objectives et le système de garantie collective qui les protège font de la Convention « l'instrument constitutionnel de l'ordre public européen » selon l'expression forte consacrée dans l'arrêt sur les exceptions préliminaires dans l'affaire *Loizidou* (315). Sachant que cette

(310) On trouvera dans H. DIPLA, *La responsabilité de l'Etat pour violation des droits de l'homme — Problèmes d'imputation*, Paris, Pedone, 1994, une excellente mise en regard des projets de la CDI et de la pratique de la Cour de Strasbourg jusque 1993.

(311) Voyez dans l'ensemble la communication de G. COHEN-JONATHAN sur « La responsabilité pour atteinte aux droits de l'homme », in *La responsabilité dans le système international*, colloque du Mans de la Société Française du Droit International, Paris, Pedone, 1991, pp. 101-135.

(312) Sur la question de l'objectivité des obligations dans les instruments internationaux de protection des droits de l'homme : J.F. FLAUSS, « La protection des droits de l'homme et les sources du droit international », in *La protection des droits de l'homme et l'évolution du droit international*, colloque de Strasbourg de la S.F.D.I., Paris, Pedone, 1998, pp. 24-28. Comp. avec la formulation du Comité des droits de l'homme qui estime que « les droits énoncés dans le Pacte constituent des normes minimales que tous les Etats parties ont accepté de respecter » (décision du 23 juillet 1999, com. n° 768/1997, *Mukunto c. Zambie*, point 6).

(313) Comm.eur.d.h., décision du 11 janvier 1961, req. n° 788/60, *Autriche c. Italie*, Ann. C.E.D.H. 1961, p. 141.

(314) Arrêt *Irlande c. Royaume Uni* du 18 janvier 1978, § 239. Quel que soit le comportement reproché, c'est toujours la théorie de l'organe qui trouve à s'appliquer, directement si l'acte internationalement illicite a été commis par l'Etat auquel il est reproché et également, mais dans un second temps, si l'illicite résulte du comportement adopté par une personne tierce sur le territoire dudit Etat.

(315) Arrêt *Loizidou c. Turquie* du 23 mars 1995 sur les exceptions préliminaires, § 75. Lisez surtout F. SUDRE, « Existe-t-il un ordre public européen ? », in P. TAVERNIER (dir.), *Quelle Europe pour les droits de l'homme ?*, Bruxelles, Bruylant, 1996, pp. 39-80.

affaire avait trait aux actes des forces armées turques en-dehors du territoire national, le principe n'en acquiert que plus d'importance.

58. Des obligations objectives de vigilance applicables sur un « territoire » de la Convention sans cesse élargi dans lequel l'Etat reste tenu de ses faits propres — Désireux de dénoncer une

« 'collusion' du silence — un vide juridique au sein des Etats membres du Conseil de l'Europe — avec son cortège de délocalisation et de sous-traitance des violations »,

le professeur Decaux concluait prémonitoirement son étude sur le « territoire des droits de l'homme » en notant que

« les différentes formes de coopération intergouvernementale comme la coopération policière (...) offrent toute une gradation de situations conflictuelles potentielles, où les Etats membres du Conseil de l'Europe seront directement ou indirectement en cause ».

En effet,

« c'est l'existence d'une communauté internationale des Etats que ce soit à travers des 'directoires internationaux de fait' ou plus légitimement à travers des organisations internationales représentant 'une très large majorité de la communauté internationale' qui entraîne des compétences fonctionnelles venant se superposer aux compétences territoriales et aux relations horizontales des Etats. Un nouvel espace, virtuel celui-là, doit être pleinement pris en compte » (316).

L'auteur a établi une distinction utile entre « compétence extra-territoriale interne » (dans l'espace de la Convention, c'est-à-dire sur l'ensemble des territoires des Etats parties) et « compétence extra-territoriale externe » (en-dehors de cet espace). Cette distinction doit être complétée par des « compétences fonctionnelles » tenant tout à fait classiquement au regard du droit de la responsabilité internationale des Etats au contrôle qu'exerce un Etat sur ses organes où qu'ils se situent. Ces règles permettent d'appréhender les responsabilités de ceux qui participent à Echelon.

L'ancienne Commission et la Cour européennes des droits de l'homme ont eu l'occasion à plusieurs reprises de se pencher sur la compatibilité avec la Convention d'actes étatiques à portée inter — ou transnationale ou encore transfrontalière (c'est selon) (317). Leur jurisprudence porte certes moins sur l'imputabilité du fait internationalement illicite que sur l'extension du

(316) Ces passages dont l'ordre a été ici inversé pour la clarté du propos sont tirés d'E. DECAUX, « Le territoire des droits de l'homme », in *Mélanges M.A. Eissen*, Bruxelles et Paris, Bruylant et L.G.D.J., 1995, pp. 77 et 78.

(317) Sur l'apport de la Cour au droit de la responsabilité internationale : J.G. MERRILLS, *The development of international law by the European Court of Human Rights*, Manchester University Press, 1988, pp. 100-103. G. COHEN-JONATHAN, « Le rôle des principes généraux dans l'interprétation et l'application de la Convention européenne des droits de l'homme », in *Mélanges L.E. Petit*, Bruxelles, Bruylant, 1998, p. 172 en vient à se demander si, vu sa jurisprudence abondante, notamment en matière d'imputabilité, ce n'est pas la Cour elle-même qui influence le droit international.

champ d'application matériel et procédural des obligations portées par la Convention (318). En effet, les règles d'imputabilité, même si leur application est souvent novatrice, restent d'inspiration tout à fait traditionnelle, l'Etat ne pouvant être tenu pour responsable que du fait de ses organes. Mais la jurisprudence strasbourgeoise n'a nullement hésité à procéder à l'imputabilité de tels manquements dans des affaires trouvant leur origine dans des rapports entre particuliers ou dans la manière dont un Etat mène ses relations internationales.

La Convention trouve en effet à s'appliquer également dans les cas où il s'agit d'apprécier la conformité avec elle des actes d'un Etat Partie posés, même par voie conventionnelle (319), dans le cadre de ses relations avec d'autres sujets de droit international, Etats ou organisations internationales. Et ce parce que l'Etat reste tenu de ses actes et omissions propres au regard de la Convention européenne des droits de l'homme laquelle, de par son article 53, a primauté sur ses autres engagements internationaux s'ils s'avèrent moins protecteurs des droits et libertés qu'elle garantit (320). La Convention, en raison de la primauté que sous-tend sa nature particulière, doit donc l'emporter sur les autres engagements internationaux des Etats parties, y compris lorsque les engagements ont été passés avec des Etats tiers (321). Un ensemble de préceptes qui s'appliquent aussi aux Etats parties qui participent à Echelon.

b) *L'imputabilité des actes et omissions « transnationaux » des Etats dans la jurisprudence de la Cour européenne des droits de l'homme*

59. Diverses hypothèses d'imputabilité ont été développées par la jurisprudence de la Cour européenne des droits de l'homme. Même dans la conduite de ses relations internationales, un Etat reste tenu de ses faits propres au regard de la Convention dont le « territoire » de la protection

(318) La jurisprudence strasbourgeoise « témoigne d'un élargissement potentiel du champ d'application territorial de nombreuses règles primaires dont on aurait pu penser qu'elles s'appliquaient exclusivement sur le territoire lui-même. Il s'agissait certes, dans chaque cas de définir le contenu de la règle primaire en cause ou de l'interpréter, et non de dégager une règle secondaire de responsabilité. Il pourrait être utile de mentionner cette évolution (...) » (J. CRAWFORD, *Deuxième rapport sur la responsabilité internationale des Etats*, présenté lors de la 51^e session de la C.D.I., A/CN.4/498, pp. 68-69). Egalement M. KAISER, « Les conditions formelles de recevabilité du recours », in *Les exceptions préliminaires dans la Convention européenne des droits de l'homme*, Bruxelles, Bruylant et Nemesis, 1997, pp. 20-22.

(319) Dans l'arrêt *Soering c. Royaume Uni* du 7 juillet 1989 par exemple, les engagements contractés dans la Convention par le Royaume Uni ont primé sur ceux passés par le Traité d'extradition de 1975 avec les Etats Unis.

(320) V. COUSSIRAT-COUSTÈRE, « Convention européenne des droits de l'homme et droit interne : primauté et effet direct », in *La Convention européenne des droits de l'homme*, Bruxelles, Nemesis, 1992, pp. 18-19.

(321) Voyez tout spécialement l'étude de G. COHEN-JONATHAN, « Les rapports entre la Convention européenne des droits de l'homme et les autres traités conclu par les Etats parties », in *Essays in Honour of H.G. SCHERMERS*, III, Dordrecht, Martinus Nijhoff, 1993, pp. 79-111.

qu'elle offre est sans cesse plus étendu. Ce principe fondamental a été vérifié dans plusieurs affaires ne se déroulant pas intégralement sur le territoire de l'Etat partie à la Convention concernée. La Cour a établi l'imputabilité d'agissements d'un Etat partie commis en territoire étranger (II.A.2.b.1). Elle en fait de même, dans les cas de « violation flagrante », à propos d'« exportations » ou d'« importations » de faits dont l'exécution est potentiellement contraire à la Convention (II.A.2.b.2). La Cour est allée jusqu'à rendre responsables les Etats parties de leur participation à l'exécution des normes d'une organisation aussi intégrée que l'Union européenne (II.A.2.b.3).

1. *L'imputabilité à l'Etat du fait de ses organes, même commis sur un territoire étranger*

60. Un cas classique de responsabilité internationale permettant de rencontrer la plupart des problèmes d'imputabilité posés par Echelon — L'extension de la juridiction au-delà du territoire national peut tout simplement résulter de la théorie classique de l'organe :

« le terme 'juridiction' ne se limite pas au territoire national des Hautes Parties Contractantes : leur responsabilité peut entrer en jeu en raison d'actes émanant de leurs organes et déployant leurs effets en-dehors dudit territoire » (322).

La responsabilité internationale est encourue pour un fait propre à l'Etat défendeur, comme cela fut jugé à propos des agissements des forces armées turques dans le nord de Chypre (323). Comme rappelé plus haut, les agents des services de renseignement d'un Etat partie qui opèrent sur une base située à l'étranger peuvent donc engager sa responsabilité internationale.

De toute façon, si des interceptions téléphoniques peuvent affecter les droits de toute personne se trouvant à l'étranger, le point de départ des interceptions est situé là où sont établies des bases de contrôle des satellites et les stations d'écoute, c'est-à-dire, en ce qui concerne le volet européen d'Echelon, au moins sur les territoires allemand (base US de Bad Aibling) et britannique (base UK de Morwenstowe, base US-UK de Menwith Hill).

Une interception transfrontalière relève par conséquent à la fois de la « compétence territoriale » classique par son origine et de la « compétence

(322) Arrêt *Drozdz et Janousek c. Espagne et France* du 26 juin 1992, § 91.

(323) Arrêt sur les exceptions préliminaires dans l'affaire *Loizidou c. Turquie* du 23 mars 1995, § 62. La Cour a cependant plutôt basé son raisonnement sur le fait que la Turquie exerçait un contrôle sur le territoire, ce qui enlève un peu au caractère opératoire de la Convention. En effet, la théorie de l'organe découle des articles 5 et suivants du projet sur la responsabilité internationale de la C.D.I.; elle permettrait de rencontrer certaines hypothèses nées de l'envoi de troupes en-dehors du territoire de la Convention; cette théorie a de surcroît été envisagée par la Commission à propos de l'éventuelle imputabilité à l'Allemagne des agissements de ses agents consulaires au Maroc, même si l'article 1^{er} de la Convention n'emporte pas un droit à la protection diplomatique pour le ressortissant d'un Etat Partie qui se trouve sur un territoire tiers (décision du 5 octobre 1984, req. n° 10686/83, D.R. 40, p. 296).

extra-territoriale interne », dans l'espace de la Convention, par son aboutissement. La « juridiction » au sens de l'article 1^{er} de la Convention de l'Allemagne et du Royaume Uni pourrait ainsi être établie sur ce double fondement puisque, dans l'hypothèse où ces pays auraient un rôle simplement passif dans Echelon, c'est leur territoire qui fournit l'instrument de la violation du droit au respect de la vie privée. Dans l'hypothèse d'une participation plus active, comme cela semble bien être le cas du Royaume Uni, la « juridiction » peut également être établie en raison de la théorie de l'organe, que ce soit sur le territoire anglais ou sur un territoire tiers où cet Etat exploiterait une autre base d'interception (l'existence d'une station = Chypre étant souvent mentionnée).

2. *L'imputabilité à l'Etat d'« importations » ou d'« exportations » de faits de nature à violer la Convention de façon « flagrante »*

61. L'imputabilité à l'Etat d'« importations » ou d'« exportations » de violations de la Convention étend considérablement le champ d'application de celle-ci — L'élément d'extranéité de la violation alléguée peut également résulter d'un mouvement d'« exportation », lorsque l'Etat Partie pose un acte qui expose une personne à une possible violation de la Convention bien que le risque se déploie sur le territoire d'un Etat tiers. Ainsi, depuis l'arrêt *Soering*, le risque de mauvais traitements qu'en court une personne dont est projetée l'extradition vers un pays qui exécute la peine de mort après un long délai d'attente dans les « couloirs de la mort », fait endosser une responsabilité à l'Etat extradant si celui-ci procédait à l'extradition. En effet,

« (...) pareille décision peut soulever un problème au regard de l'article 3, donc engager la responsabilité d'un Etat contractant au titre de la Convention, lorsqu'il y a des motifs sérieux et avérés de croire que l'intéressé, si on le livre à l'Etat requérant, y courra un risque réel d'être soumis à la torture, ou à des peines ou traitements inhumains et dégradants. Pour établir une telle responsabilité, on ne peut éviter d'apprécier la situation dans le pays de destination à l'aune des exigences de l'article 3. Il ne s'agit pas pour autant de constater ou prouver la responsabilité de ce pays en droit international général, en vertu de la Convention ou autrement. Dans la mesure où une responsabilité se trouve ou peut se trouver engagée sur le terrain de la Convention, c'est celle de l'Etat contractant qui extradé, à raison d'un acte qui a pour résultat direct d'exposer quelqu'un à des mauvais traitements prohibés » (324).

(324) Arrêt *Soering c. Royaume Uni* du 7 juillet 1989, § 91 et les commentaires de W.J. GANS-HOF VAN DER MEERSCH, « L'extradition et la Convention européenne des droits de l'homme », *R.T.D.H.* 1990, pp. 22-23. Ultérieurement, voyez notamment les arrêts *Cruz Varos et autres c. Suède* du 20 mars 1991, §§ 69 et 70, et *Vilvarajah et autres c. Royaume Uni* du 30 octobre 1991, § 103. L'arrêt *Chahal et autres c. Royaume-Uni* du 15 novembre 1996, § 74, a confirmé cette jurisprudence et a jugé que la circonstance que la personne dont l'extradition est demandée soit considérée par l'Etat extradant comme un terroriste mettant en danger sa sécurité nationale est indifférente pour apprécier s'il y a ou non violation de la Convention (§§ 75-82). En tout dernier lieu, arrêt *Jabari c. Turquie* du 11 juillet 2000, § 38.

Il y a ici aussi responsabilité internationale pour fait propre puisque l'origine de la violation se situe dans la juridiction de l'Etat partie (325).

L'élément d'extranéité de la violation alléguée peut, en sens inverse, résulter d'un mouvement d'« importation » d'un acte étranger sur le territoire national, lorsqu'il s'agit d'en apprécier la validité dans l'ordre juridique national. C'est le cas, par exemple dans les affaires d'enlèvements à l'étranger de personnes amenées, plus ou moins officiellement, sur le territoire national pour y être détenues ou jugées (326). Des situations plus fréquentes ont lieu en matière d'exécution des jugements étrangers en droit international privé ou lorsqu'il s'agit de donner effet à une loi étrangère sur le territoire national, le juge du for se posant la question de savoir si la Convention fait partie de l'ordre public international qui lui permet d'écarter la règle étrangère ou conventionnelle si elle est en contrariété avec un droit garanti par la Convention (327).

L'Etat encourt aussi en de telles occasions une responsabilité internationale pour un fait propre de ses organes. L'affaire *Droz et Janousek contre Espagne et France* en fournit une illustration. En l'occurrence, des personnes condamnées à une peine de détention à Andorre contestaient leur transfèrement en France pour y purger leur peine. La Cour, sévèrement critiquée sur ce point par l'opinion dissidente d'une forte minorité craignant le développement de zones de « non-droit », commença par estimer que la Convention était inapplicable à Andorre qui n'y était pas partie. Néanmoins,

« ce constat ne dispense pas la Cour de rechercher si des requérants ont relevé de la 'juridiction' de la France ou de l'Espagne, au sens de l'article 1er de la Convention, en raison de leur condamnation par un tribunal andorran » (328).

Rappelant la jurisprudence précitée selon laquelle un Etat peut engager sa responsabilité pour des faits déployant leurs effets en-dehors du territoire, la Cour jugea que même si la France et l'Espagne avaient mis à disposition d'Andorre des magistrats, ceux-ci avaient agi en qualité d'organes de la principauté; leurs jugements n'étaient donc imputables à aucun de ces

(325) Moyennant la preuve par celui qui conteste son extradition qu'il encourt un risque réel de violation de ses droits, le Comité des droits de l'homme estime aussi que « les Etats parties doivent s'acquitter de tous leurs engagements juridiques, qu'ils relèvent de la législation nationale ou d'accords conclu avec d'autres Etats, d'une manière qui soit compatible avec le Pacte » : décision du 28 juillet 1997, com. n° 692/1996, *A.R.J. c. Australie*, point 6.8. Sur la primauté du Pacte, également la décision du 20 octobre 1998, com. n° 628/1995, *Tae Hoon Park c. Corée du Sud*, point 10.4.

(326) Le principe « *male captus, bene detentus* » est contesté au regard de la Convention dans une étude au titre très évocateur de J.A. FROWEIN, « Male Captus Male Detentus — a Human Right », in. *Essays in honour of H.G. SCHERMERS*, III, Dordrecht, Martinus Nijhoff, 1993, p. 184.

(327) P. COURBE, « Le droit international privé et les difficultés d'insertion de la Convention dans le système français », in P. TAVERNIER (dir.), *Quelle Europe pour les droits de l'homme?*, Bruxelles, Bruylant, 1996, pp. 249-267; P. MAYER, « La Convention européenne des droits de l'homme et l'application des normes étrangères », *R.C.D.I.P.* 1991, p. 651.

(328) Arrêt *Droz et Janousek*, § 90.

deux pays. Restait la question du contrôle par les juridictions françaises de la condamnation litigieuse et de l'éventuelle responsabilité de la France. Pour la Cour,

« la Convention n'obligeant pas les Parties contractantes à imposer ses règles aux Etats ou territoires tiers, il n'incombait pas à la France de rechercher si la procédure qui déboucha sur cette condamnation remplissait chacune des conditions de l'article 6 [droit à un procès équitable]. Exiger un tel contrôle de la manière dont une juridiction non liée par la Convention applique les principes se dégageant de ce texte contrecarrerait aussi la tendance actuelle au renforcement de l'entraide internationale dans le domaine judiciaire, tendance normalement favorable aux intéressés ».

Mais la Cour termine son raisonnement en affirmant que

« les Etats contractants doivent toutefois se garder d'apporter leur concours s'il apparaît que la condamnation résulte d'un déni de justice flagrant » (329).

62. Un Etat participant à Echelon apporte son concours à une violation flagrante de la Convention — La Commission européenne des droits de l'homme a estimé irrecevables des requêtes dirigées contre le refus par des juridictions internes de poser une question préjudicielle à la Cour de justice des Communautés européennes tant que celles-ci ne sont pas parties à la Convention. Mais la Commission a tout aussi clairement réservé l'hypothèse des refus qui seraient manifestement arbitraires; en pareil cas, les organes de la Convention devraient quand même examiner la requête (330).

Pour résumer le propos qui concerne ici des cas de « compétence extra-territoriale externe », c'est-à-dire des hypothèses de violation perpétrées ou pouvant se perpétrer en-dehors de l'espace de la Convention, on retiendra donc que

« en cas de violation flagrante et manifeste déjà commise ou de risque réel de violation, appuyé par des motifs sérieux de croire à son existence, la Cour prescrit que les Etats doivent se garder d'apporter leur concours soit en permettant l'accomplissement de l'acte en cause, soit en lui donnant effet dans leur propre ordre juridique » (331).

La jurisprudence strasbourgeoise enseigne donc que dans de tels cas complexes de mise en œuvre de la responsabilité d'Etats parties dans leurs rela-

(329) Arrêt *Drozd et Janousek*, § 110. Sur cette affaire : G. COHEN-JONATHAN et J.F. FLAUS, « Convention européenne des droits de l'homme et exécution des condamnations pénales prononcées à l'étranger », *R.T.D.H.* 1994, pp. 98-115.

(330) Comm.eur.d.h., décision du 12 mai 1993, req. n° 20631/92, *Société Divagsa c. Espagne*, D.R. 74, p. 277. Egalement la décision du 28 juin 1993, req. n° 15669/89, *F.S. et N.S. c. France*, D.R. 75, p. 39. A ce sujet : G. COHEN-JONATHAN, « La Commission européenne des droits de l'homme et le droit communautaire : quelques précédents significatifs », *Europe*, décembre 1994, p. 4; O. DE SCHUTTER et J. FIERENS, « Examen de jurisprudence — Convention européenne des droits de l'homme (1992-1993) », *J.T.D.E.* 1993, p. 72; F. SUDRE, « La Communauté européenne et les droits fondamentaux après le Traité d'Amsterdam », *Sem.Jur.* 1998, doc. 100.

(331) P. APRAXINE, « Violation des droits de l'homme par une organisation internationale... », *op. cit.*, pp. 27-28.

tions avec des Etats tiers, le contrôle de conformité des actes imputables aux Etats parties avec la Convention est atténué par rapport au contrôle opéré en temps normal dans les relations existant entre seuls Etats parties ou entre un de ceux-ci et une personne relevant de sa juridiction (332). Mais il n'en demeure pas moins que, même réservé à des cas de violation flagrante de la Convention, un tel contrôle existe et doit être opéré.

Or, les conditions d'une violation manifeste, flagrante et massive de la Convention semblent bel et bien réunies si l'on a égard à la « philosophie » du programme Echelon qui consiste à mener, de manière exploratoire et indifférenciée, à très grande échelle la captation de toutes les conversations téléphoniques qui contiennent certains mots-clés parfaitement inconnus, en violation avec les exigences de prévisibilité et d'accessibilité minimales que même les mécanismes de surveillance secrète doivent présenter pour être conformes avec le droit eu respect de la vie privée et de la correspondance. Si ces règles de fond portées par la jurisprudence de la Cour sont violées, il ne s'agit pas ici de seulement mesurer comment doit être engagée la « compétence extra-territoriale externe » découlant des rapports d'Etats Parties avec des Etats tiers; il s'agit bel et bien aussi d'envisager comment un Etat peut être tenu responsable de son défaut de vigilance quant au comportement des organes d'un Etat étranger valablement accueillis sur son territoire, c'est-à-dire de déterminer comment est engagée une « compétence territoriale » on ne peut plus classique.

La responsabilité en raison de la « compétence extra-territoriale externe » permet aussi de répondre à l'éventuel argument selon lequel, les interceptions des communications par satellite ayant lieu dans l'espace extra-atmosphérique, qui n'est soumis à aucune souveraineté, se situeraient en-dehors du champ d'application spatial de la Convention. Qui plus est, le rapatriement sur Terre du fruit de ces interceptions aboutit forcément sur un territoire national quelconque. Si c'est sur la base de Menwith Hill, par exemple, étant à la fois cogérée par les anglais et située sur le territoire anglais, ce sont respectivement la théorie de l'organe et la compétence territoriale qui entrent à nouveau en jeu.

L'applicabilité de la Convention à l'aide de la « compétence extra-territoriale externe » offre ainsi la possibilité d'établir l'imputabilité à un Etat

(332) Dans son article précité sur « Les rapports entre la Convention européenne des droits de l'homme et les autres traités conclus par les Etats parties », Gérard COHEN-JONATHAN plaide aussi en faveur de l'effet « atténué » de la Convention lorsqu'il s'agit d'exécuter une norme étrangère ou découlant d'un accord conclu avec un Etat tiers, d'une part, et pour ne contrôler que les cas de violation les plus graves lorsqu'il s'agit de refuser une extradition, d'autre part. La théorie de l'effet atténué ne nous convainc pas plus que le professeur SUDRE qui parle même de l'effet « anéanti » (« Existe-t-il un ordre public européen? », *op. cit.*, p. 79). Il semble d'ailleurs que l'arrêt *Matthews* (analysé au n° 65) ne comporte plus de telle distinction. De toute façon (la jurisprudence de la Cour étant ce qu'elle est), le caractère massif et systématique des violations de l'article 8 ici alléguées n'est pas de nature à remettre en cause la primauté que doit recevoir la Convention sur tout autre engagement contracté par l'Allemagne et le Royaume-Uni.

partie à la Convention de faits éventuellement générés, initialement ou potentiellement, dans ou par un autre Etat qui, comme les Etats Unis, n'y serait pas partie.

3. *L'imputabilité à l'Etat du fait de l'exécution des normes d'une organisation internationale*

63. Même si l'accord UKUSA instituait une organisation internationale, les Etats participants resteraient responsables de leurs faits propres en relation avec celle-ci — L'élément international de la violation alléguée peut enfin résulter de la manière dont un Etat conduit ses relations internationales sur son territoire, quand l'acte reproché tient au fait propre de l'Etat dans ses relations avec une organisation internationale ou un Etat tiers, dans le cadre de relations conventionnelles ou non.

Echelon ne paraît pas avoir été créé ni mené dans le cadre d'une organisation internationale dotée de la personnalité juridique; si c'était toutefois le cas, les développements exposés ici se justifieraient également. Il s'agit, d'après ce que l'on peut en savoir, tout au plus de la mise en place d'une structure de surveillance électronique dans le cadre de l'accord UKUSA de 1947 (ou 1948) dont, à part les cinq pays anglo-saxons (dont le Royaume Uni) qui en constituent la charpente, les parties tierces (à part le Japon et spécialement l'Allemagne) ne sont pas toutes connues.

Ce qui justifie avant tout l'analyse de la jurisprudence sur les relations qu'entretient un Etat avec une organisation internationale, aux termes d'un acte de siège ou de son traité constitutif, réside cependant dans l'affirmation solennelle par la Cour européenne des droits de l'homme de la primauté de la Convention sur tout autre engagement international de l'Etat. La Cour a certes déjà fait prévaloir la Convention sur d'autres traités, y compris ceux passés par exemple en matière d'extradition par un Etat partie avec un Etat tiers; le principe ne pose pas problème. Mais c'est pourtant à propos de la responsabilité internationale des Etats parties dans leurs rapports avec une organisation internationale aussi intégrée que l'Union Européenne que la Cour a appliqué avec une force sans égale la portée, très étendue, du principe de la primauté de la Convention sur tout acte moins protecteur des droits qu'elle garantit.

L'Etat, cela a été dit plus haut, demeure astreint par le droit des gens au respect, qui lui incombe en propre, d'une obligation de vigilance à l'égard des activités de personnes internationales qui se déroulent sur son territoire. Il n'y sera pas revenu, la règle demeurant parfaitement valable quand une organisation internationale est concernée (333).

(333) Voyez tout particulièrement l'analyse de la jurisprudence de la Commission européenne des droits de l'homme à propos des Communautés Européennes à laquelle procède P. KLEIN, *La*

Mais, même membre d'une organisation internationale, l'Etat reste par ailleurs tenu de ses faits propres quand bien même ils seraient en rapport avec un acte de cette organisation. C'est très certainement la position de la Cour qui contrôle désormais les actes nationaux d'exécution du droit communautaire (334). Et quelles que soient les critiques dont la jurisprudence de l'ancienne Commission européenne des droits de l'homme a pu faire l'objet quant à l'application dans certains cas d'espèce de la règle qu'elle a dégagée, ces critiques ne portaient pas sur la validité de ce précepte sans équivoque (335) :

« la Convention n'interdit pas à un Etat membre de transférer des pouvoirs à des organisations internationales. Néanmoins, la Commission rappelle que 'si un Etat assume des obligations contractuelles et conclut par la suite un autre accord international qui ne lui permet plus de s'acquitter des obligations qu'il a assumées par le premier traité, il encourt une responsabilité pour toute atteinte portée de ce fait aux obligations qu'il assumait en vertu du traité antérieur' » (336).

64. L'arrêt *Matthews* a affirmé la primauté de la Convention sur toute autre norme interne ou internationale — L'arrêt *Matthews contre Royaume-Uni*, rendu le 18 février 1999 à propos de la non-organisation des élections pour le Parlement européen sur le territoire de Gibraltar, a exprimé avec clarté et audace la manière dont la Cour entend voir mise en œuvre la responsabilité internationale des Etats parties en matière de

responsabilité des organisations internationales dans les ordres juridiques internes et en droit des gens, Bruxelles, Bruylant, 1998, pp. 470-480.

(334) Solution implicite dans l'ensemble de l'arrêt *Van de Hurk c. Pays-bas* du 19 avril 1994 dans une affaire de dépassement de quotas laitiers imposés par un règlement CEE. Cette position est explicitée dans l'arrêt *Procola c. Luxembourg* du 28 septembre 1995, toujours à propos de quotas laitiers. Elle est certainement incontestable depuis l'arrêt *Hornsby* du 19 mars 1997 qui a condamné la Grèce en raison du retard mis par ses autorités administratives dans l'exécution d'un arrêt du Conseil d'Etat consécutif à une question préjudicielle de la C.J.C.E.

(335) Comm.eur.d.h., décision du 9 février 1990, req. n° 13258/87, *M. & Co c. R.F.A., R.U.D.H.* 1991, p. 134. Parmi beaucoup de commentaires : A. CLAPHAM, « A Human rights policy for the European Community », *Y.E.L.* 1990, spéc. pp. 332-335 ; F. RIGAUX, « L'article 192 du Traité CEE devant la Commission européenne des droits de l'homme », *R.T.D.H.* 1991, pp. 398-402 ; H.G. SCHERMERS, « The European Communities bound by fundamental human rights », *C.M.L.R.* 1990, pp. 249-258 ; L. WEITZEL, « La Commission européenne des droits de l'homme et le droit communautaire », *Mélanges J. Velu*, t. III, Bruxelles, Bruylant, 1992, pp. 1391-1406 et les références nombreuses à des décisions inédites ; J. ZDZOJEWSKI, C. et L. PETTTI, « Une décision à points d'interrogations sur les rapports Communauté économique européenne et Conseil de l'Europe », *Gaz. Pal.* 1990, doc., p. 346.

(336) La jurisprudence de la Commission est constante : décision du 10 juin 1958, req. n° 235/56, *X. c. R.F.A., Ann.C.E.D.H.*, 1958-1959, p. 301 ; décision du 3 juin 1960, req. n° 655/59, *X. c. R.F.A., Rec.* 4, p. 4 ; décision du 9 décembre 1987, req. n° 11123/84, *Tête c. France, D.R.* 54, p. 59 ; décision du 10 mars 1988, req. n° 11406/85, *Fournier c. France, D.R.* 55, p. 134. La décision *M. & Co* alla même plus loin en affirmant que « le transfert de pouvoirs à une organisation internationale n'est pas incompatible avec la Convention, à condition que, dans cette organisation, les droits fondamentaux reçoivent une protection équivalente », condition qui n'a pas été reprise dans des affaires ultérieures (comparez avec le § 32 de l'arrêt *Matthews* du 18 février 1999 qui demande que ces droits continuent à être « reconnus »). Le conflit éventuel entre la Convention et le Traité UKUSA de 1947 auquel le Royaume Uni est partie ne peut être ici réglé en fonction des règles d'antériorité et de postériorité. La Convention prévaut en vertu de son article 53 puisque, par hypothèse plus que raisonnable, elle est plus protectrice des droits fondamentaux.

droits fondamentaux, même lorsqu'ils sont parties à d'autres traités internationaux et même si ces traités sont constitutifs d'une organisation internationale :

« § 29 — [L'article 1^{er}] ne fait aucune distinction quant au type de normes ou de mesures en cause et ne soustrait aucune partie de la 'juridiction' des Etats membres à l'empire de la Convention (arrêt Parti Communiste Unifié de Turquie et autres c. Turquie du 30 janvier 1998).

§ 32 — (...) Les actes de la Communauté européenne ne peuvent être attaqués en tant que tels devant la Cour, car la Communauté en tant que telle n'est pas Partie contractante. La Convention n'exclut pas le transfert de compétences à des organisations internationales pourvu que les droits garantis par la Convention continuent d'être 'reconnus'. Pareil transfert ne fait donc pas disparaître la responsabilité des Etats membres.

§ 33 — (...) Le Royaume-Uni, conjointement avec l'ensemble des autres parties au Traité de Maastricht, est responsable *ratione materiae* au titre de l'article 1^{er} de la Convention et, en particulier de l'article 3 du Protocole n° 1, des conséquences de ce traité » (337).

L'arrêt *Beer et Regan contre Allemagne*, rendu le même jour à propos de l'immunité de juridiction de l'Agence Spatiale Européenne sur le territoire allemand (338), a également invoqué la règle de la primauté de la Convention :

« lorsque des Etats créent des organisations internationales pour coopérer dans certains domaines d'activité ou pour renforcer leur coopération, et qu'ils transfèrent des compétences à ces organisations et leur accordent des immunités, la protection des droits fondamentaux peut s'en trouver affectée. Toutefois, il serait contraire au but et à l'objet de la Convention que les Etats contractants soient ainsi exonérés de toute responsabilité au regard de la Convention dans le domaine d'activité concerné. Il y a lieu de rappeler que la Convention a pour but de protéger des droits non pas théoriques ou illusoire, mais concrets et effectifs » (339).

(337) Il est très intéressant de noter que dans ses moyens de défense soulevés devant la Cour, le Royaume-Uni a reconnu que « il pourrait y avoir des circonstances où une Partie contractante pourrait enfreindre ses obligations au titre de la Convention en souscrivant par voie de traité des obligations incompatibles avec cet instrument » (arrêt *Matthews c. Royaume-Uni* du 18 février 1999, § 26).

(338) Comm.eur.d.h., décision du 12 décembre 1988, req. n° 12516/86, *Spaans c. Pays-Bas*, DR 58, p. 119 jugeait encore qu'il n'est pas contraire à l'article 1^{er} de la Convention qu'un Etat accorde à une institution internationale une immunité de juridiction qui fait échapper aux tribunaux nationaux les litiges entre cette institution et son personnel.

(339) Arrêt *Beer et Regan c. Allemagne* du 18 février 1999, § 57 ainsi que la même solution, le même jour, dans l'arrêt *Wait et Kennedy c. Allemagne*. Il s'agissait en l'occurrence d'apprécier la conformité de l'immunité de juridiction de l'Agence Spatiale Européenne avec l'article 6 de la Convention qui garantit le droit à un procès équitable dans un litige l'opposant à certains de ses employés. La Cour procéda au contrôle de la proportionnalité de cette limitation du droit d'accès à un tribunal en établissant que les travailleurs disposaient des recours *ad hoc* au sein de l'ASE et que celle-ci ne pouvait être tenue d'appliquer le droit allemand du travail. Voyez cependant quant à l'absence de contrôle par la Cour de cette limitation de souveraineté, les critiques de H. TIGROUDJA, « L'immunité de juridiction des organisations internationales et le droit d'accès à un tribunal », *R.T.D.H.* 2000, p. 101. J.F. FLAUS, « Contentieux de la fonction publique européenne et Convention européenne des droits de l'homme », in *Etudes à la mémoire de J. Schwob*, Bruxelles, Bruylant, 1997, p. 161 notait déjà à propos de la jurisprudence de la Commission, déclarant irrecevables *ratione materiae* les requêtes de fonctionnaires européens, que « en totale

Qui peut le plus, peut le moins. L'alliance de la primauté de la Convention et de ses obligations objectives s'impose sans conteste aussi à ses Etats parties qui collaborent sous une forme ou l'autre à Echelon.

Un Etat ne peut être tenu de tout ce qui se passe sur son territoire que le fait en cause émane d'un particulier, de l'organe d'un Etat tiers ou d'une organisation internationale. Encore faut-il qu'il ait pris toutes les précautions nécessaires pour éviter une violation de la Convention (340). Car le droit international général (obligation de vigilance sur le territoire) comme la Convention (obligations positives et de vigilance) lui imposent au minimum une obligation de moyens consistant à adopter les mesures raisonnables et appropriées de nature à éviter la violation de l'article 8 de la Convention ou sa perpétuation.

Faute pour le Royaume Uni, qui participerait à Echelon dans les conditions qui seraient celles décrites dans cette étude, d'y mettre un terme, il violerait la Convention. Faute pour l'Allemagne et le Royaume Uni d'au moins protester officiellement et publiquement contre l'usage supposé de leur territoire par des services de renseignement tiers, voire de mettre un terme à cet usage du territoire contraire à la Convention violée par une politique systématique d'écoutes massives, ces Etats parties violeraient la Convention. Cette violation découle non pas du fait de puissances tierces, même si elle y trouve matériellement son origine, mais d'un fait dûment imputable à des Parties : le manquement à un devoir de vigilance ou de diligence due.

La complexité apparente de l'établissement de l'imputabilité à des Etats Parties à la Convention peut être parfaitement démêlée en ayant recours aux mécanismes classiques de la responsabilité tels qu'ils ont déjà été appliqués à plusieurs reprises par la jurisprudence strasbourgeoise. Et ce d'autant plus que les exigences procédurales tenant à l'introduction des requêtes, étatiques ou individuelles, sont singulièrement réduites quand est contesté un système structurel et secret de surveillance.

harmonie avec la théorie des immunités, telle qu'elle est pratiquée en droit international, pareille dénégation de compétence ne tient pas cependant suffisamment compte de l'éventuelle spécificité des normes internationales relatives à la protection des droits de l'homme ». Ne contestant pas que l'utilité opératoire de sa suggestion serait marginale, l'auteur poursuivait : « *pour renforcer la territorialité de l'application de la CEDH à l'encontre d'organisations internationales, il serait aussi concevable de faire appel à l'idée de hiérarchisation des normes internationales. En d'autres termes, les règles relatives à l'immunité de juridiction devraient s'effacer devant d'éventuelles normes internationales à valeur supérieure, c'est-à-dire celles qualifiées de 'normes impératives du droit international'* » (p. 166).

(340) Arrêt *Plattform « Ärzte für das Leben »* du 21 juin 1988, § 34, à propos d'un recours contre la passivité de la police autrichienne lors de manifestations organisées par des médecins hostiles à l'avortement et perturbées par une contre-manifestation : « *s'il incombe aux Etats contractants d'adopter des mesures raisonnables et appropriées afin d'assurer le déroulement pacifique des manifestations licites, ils ne sauraient pour autant le garantir de manière absolue et ils jouissent d'un large pouvoir d'appréciation dans le choix de la méthode à utiliser. En la matière, ils assument en vertu de l'article 11 de la Convention une obligation de moyens et non de résultat* ».

B. — Les conditions des recours en manquement aux obligations portées par la Convention — Surveillance structurelle secrète, « pratiques administratives » et « victimes potentielles »

65. Particuliers et Etats ne sont pas *a priori* dans la même position lorsqu'ils souhaitent introduire un recours devant la Cour européenne des droits de l'homme pour contester des manquements à la Convention imputables à des Etats parties. Il existe en effet des conditions de recevabilité communes aux deux requêtes (II.B.1) et certaines qui sont propres aux requêtes individuelles (II.B.2). Toutefois, être confronté à un système potentiellement structurel et secret comme Echelon offre la possibilité d'invoquer des exceptions aux règles normales de procédure. Celles-ci ainsi que le degré variable d'engagement des Etats soupçonnés de participer à Echelon figurent parmi les motifs qui doivent faire préférer la Cour de Strasbourg plutôt que le Comité des droits de l'homme de l'ONU si l'on désire contester l'existence et les conséquences de ce système de surveillance électronique (II.B.3).

1. Les conditions communes de recevabilité des requêtes devant la Cour européenne des droits de l'homme contre Echelon : la non-obligation d'épuiser les voies de recours internes ni de respecter le délai de six mois en cas de « pratiques administratives »

66. La première des conditions communes de recevabilité est l'épuisement préalable des voies de recours internes (II.B.1.a.1). Ce principe fondamental du droit international général connaît plusieurs exceptions. La première pourrait se réclamer d'une partie de la jurisprudence internationale selon laquelle ne doit pas être épuisé le recours instauré par un Etat alors que la « juridiction » de celui-ci est internationalement illicite. Une autre exception à ce principe général tient dans la dispense d'actionner les recours internes inexistantes ou inefficaces. Mais l'exception la plus marquante dans le cadre d'Echelon serait peut être celle considérant ce programme d'espionnage comme étant constitutif de « pratiques administratives » (II.B.1.a.2). Le sort de la condition selon laquelle la requête doit être introduite dans un délai de six mois à dater de la décision définitive querellée (II.B.1.b.) est intimement lié à celui de la règle de l'épuisement préalable.

a) L'épuisement des voies de recours internes par les particuliers n'est pas requis en cas de « pratiques administratives »

1. L'épuisement préalable des voies de recours interne : un principe général du droit international

67. Un principe protecteur de la souveraineté étatique mais qui souffre plusieurs exceptions — Le principe de l'épuisement préalable des

voies de recours internes avant toute contestation devant un organisme international est fondamental en droit international puisqu'il vise à permettre à l'Etat visé de redresser les violations alléguées (341), ce qui implique que les griefs tirés de la violation de la Convention soient au moins invoqués en substance devant les juridictions nationales dans les formes et délais prévus par l'ordre juridique interne (342).

L'article 35 instaure une répartition de la charge de la preuve. L'exception doit être soulevée par l'Etat défendeur qui doit démontrer que les recours sont, en théorie et en pratique, effectifs et disponibles, qu'ils offrent une perspective raisonnable de succès et qu'ils peuvent redresser le grief. Cela fait, le requérant doit établir soit qu'il a employé le recours, soit qu'il n'est ni adéquat ni effectif en l'espèce, soit qu'il existe des circonstances particulières le dispensant d'exercer le recours. Il revient alors au Gouvernement défendeur de montrer quelles mesures il a prises (343).

Le principe n'en comporte pas moins plusieurs limites ou exceptions dans l'ordre juridique spécifique de la Convention :

- en cas d'inexistence d'une de voie de droit adéquate;
- en cas de non-accessibilité au requérant des voies de droit adéquates;
- en cas de toute absence de chance de succès des recours existants;
- en cas de circonstances particulières rendant impossible ou inutile le recours;
- en cas de « pratiques administratives » illicites rendant vain l'exercice de tout recours (344).

68. Les requêtes individuelles doivent *a priori* satisfaire à des conditions de recevabilité plus strictes que les requêtes étatiques —
L'article 35, § 1^{er}, de la Convention en disposant que

« la Cour ne peut être saisie qu'après l'épuisement des voies de recours des voies de recours internes, tel qu'il est entendu selon les principes de droit international généralement reconnus, et dans un délai de six mois à partir de la date de la décision définitive »,

(341) L'arrêt *Beis c. Grèce* du 20 mars 1997, § 36, a ainsi accueilli l'exception préliminaire du Gouvernement grec parce que le requérant n'avait pas épuisé les recours internes disponibles. Sur la portée de la règle de l'épuisement à propos de laquelle l'article 35, § 1^{er}, de la Convention renvoie expressément aux « principes de droit international généralement reconnus » et les tempéraments qui y sont apportés : P. TAVERNIER, « L'étendue de la compétence de l'organe de contrôle », in *L'interprétation de la Convention européenne des droits de l'homme*, Bruxelles, Nemesis et Bruylant, 1998, pp. 184-187.

(342) Pour une espèce dans laquelle la Cour a estimé que cela n'avait pas été le cas, cons. l'arrêt *Ahmet Sadik c. Grèce* du 15 novembre 1996, § 30.

(343) Sur la charge de la preuve, par exemple, arrêt *Selmouni c. France* du 28 juillet 1999, § 76.

(344) Sur toutes ces exceptions à la règle de l'épuisement préalable des voies de recours internes : E. PICARD, « Article 26 », in L.E. PETTITI, E. DECAUX et P.H. IMBERT, *La Convention européenne des droits de l'homme — Commentaire article par article*, 2^e éd., Paris, Economica, 1999, pp. 603-610.

requiert donc l'épuisement préalable tant des requêtes étatiques fondées sur l'article 33 que des requêtes individuelles fondées sur l'article 34.

Le professeur Sudre a fort bien exposé en quelques mots le moindre degré d'exigence qui pèse sur l'État requérant dans le cadre du recours étatique dès lors qu'il reproche à l'État défendeur des pratiques administratives ou l'existence d'une norme en soi contraire à la Convention :

« la règle de l'épuisement des voies de recours internes vaut pour les requêtes individuelles comme pour les requêtes interétatiques ; toutefois, pour ces dernières, cette condition (et aussi, par conséquent, celle relative au délai de six mois) ne s'applique pas si l'État demandeur dénonce, non pas des cas individuels de violation dont les victimes sont identifiées, mais l'incompatibilité avec la Convention de mesures législatives ou d'une 'pratique administrative'. La 'pratique administrative' suppose à la fois la répétition d'actes contraires à la Convention (...) et la tolérance officielle : par tolérance officielle, il faut entendre que les supérieurs immédiats des agents responsables des actes incriminés ne font pas cesser ces actes ou que l'autorité supérieure ne prend pas de mesure suffisante pour mettre fin à la répétition des actes » (345).

Se pose néanmoins la question, à laquelle est apportée ci-après une réponse affirmative, de savoir si les particuliers peuvent également se prévaloir de l'existence d'une pratique administrative pour contester que les conditions de l'épuisement des voies de recours internes et le délai de six mois leur sont opposables lorsqu'ils sont confrontés à un programme secret d'espionnage électronique comme Echelon. Ceci ne constitue cependant qu'une exception parmi d'autres qui sont également invocables par les requêtes individuelles.

2. *Les exceptions à la règle de l'épuisement préalable qui peuvent être invoquées dans le cas d'Echelon*

a. *Le caractère illicite des actes de contrainte à portée extra-territoriale que sont les interceptions téléphoniques fait que les particuliers ne sont pas valablement sous la « juridiction » des États qui y procèdent*

69. Le rappel de l'interdiction de principe des actes de contrainte extra-territoriaux — Une première raison milite contre l'application du principe de l'épuisement des voies de recours internes ; elle réside à nouveau dans le domaine d'application de la « loi » en cause.

Quand bien même les mécanismes de surveillance querellés seraient en conformité avec les droits anglais et allemands et quand bien même le programme Echelon serait-il valide, au regard du droit international entre les États qui y prennent part, ces mécanismes doivent normalement voir leur

(345) F. SUDRE, *Droit international et européen des droits de l'homme*, 4^e éd., Paris, PUF, 1999, p. 384 et la jurisprudence citée.

effets limités à leurs territoires respectifs. Ainsi le veut l'interdiction de principe des actes de contrainte extra-territoriaux ou qui ne peuvent se réclamer d'une compétence personnelle. L'incrimination extra-territoriale est une chose. Les actes de contrainte en sont une autre.

Force est cependant de constater, ou de supputer puisque c'est précisément le secret qui cause problème, que les actes en contrariété avec les droits garantis par la Convention existent. Pour un ressortissant tiers au pays qui a élaboré la législation ou qui l'applique, cette législation, dès lors que le ressortissant ne se trouve pas sur le territoire de l'État, n'en constitue pas moins pour lui un fait, voire une partie d'un ensemble plus vaste de pratiques administratives, qui constitue une ingérence ou un risque raisonnable d'ingérence dans son droit à la vie privée.

On ne peut ainsi pas déceimment requérir d'un slovaque qui a une conversation téléphonique avec un norvégien grâce à des relais situés en Autriche et au Danemark d'introduire un recours devant les juridictions anglaises ou allemandes sur base de faits qu'il ne connaît pas, de lois, si elles existent, qu'il ne connaît pas et n'a d'ailleurs pas à connaître. Le constat est identique quand un français adresse un télex à un autre français en France ou quand un belge envoie un courrier électronique à un néerlandais en vacance en Suisse qui le faxe à son tour à son neveu résidant en Pologne.

Il pourrait donc être plaidé que les requérants individuels qui ne tombent pas valablement sous la juridiction de l'État qui viole la Convention n'ont pas à épuiser les voies de recours internes que le droit de cet État a mises en place.

En d'autres termes, si la notion de « juridiction » portée par l'article 1^{er} de la Convention doit certainement s'entendre au sens large pour déterminer qu'un État la viole, comme en atteste la jurisprudence de la Cour recensée dans la deuxième partie à propos des actes « transnationaux », la protection qu'il convient d'accorder aux particuliers dans les circonstances très particulières des programmes d'espionnage électronique appellerait tout autant une interprétation étroite de cette même notion de « juridiction » lorsqu'il s'agit de constater l'impossibilité, tant matérielle que juridique, de mettre en œuvre les voies de recours organisées par le droit national du ou des États qui procèdent aux écoutes et interceptions et ce, parce que ladite juridiction n'est pas valable au regard du droit international général. En d'autres mots encore, l'interprétation extensive de la « juridiction » sur le plan matériel s'imposerait dans les circonstances présentes pour déterminer l'existence de victimes au nom du caractère concret et effectif des droits et obligations contenus dans la Convention ; mais l'interprétation restrictive de la « juridiction » s'imposerait sur le plan procédural d'un autre côté quand le titre sur lequel elle repose n'a manifestement aucun fondement valable au regard du droit international.

70. Certaines décisions strasbourgeoises semblent relever le demandeur de l'obligation de l'épuisement quand l'Etat défendeur n'a pas de titre de juridiction valable — C'est en ce sens, semble-t-il, que la Commission s'est prononcée dans une des affaires *Chypre contre Turquie* en estimant d'abord que

« la règle de l'épuisement des voies de recours internes ne s'applique pas aux griefs tendant à faire statuer sur la compatibilité avec la Convention de mesures législatives et de pratiques administratives (...) sauf lorsqu'il existe des voies de recours spécifiques et efficaces contre lesdites mesures ».

En l'occurrence,

« les voies de recours internes qui, selon le Gouvernement défendeur, peuvent être exercées devant les tribunaux internes turcs, ne peuvent, sous l'angle des présents griefs relatifs à la violation des droits de l'homme des Chypriotes grecs à Chypre, être considérées comme 'à la fois accessibles et efficaces' » (346).

Cette thèse pourrait également trouver appui dans l'arrêt *Aksoy contre Turquie* où la Cour mit en avant une autre circonstance particulière de nature à relever de l'obligation d'épuiser les voies de recours internes (347).

On pourrait en inférer qu'un requérant qui se plaint d'un manquement commis par un autre pays que celui dont il relève par ailleurs valablement en droit international (au titre de la compétence territoriale ou de la compétence personnelle) n'aurait donc pas à épuiser les voies de recours internes ni de son pays, dans la mesure où celui-ci n'a pas favorisé ou participé au manquement querellé (348), ni de l'autre pays, puisque ce dernier n'a aucun titre valable de juridiction à faire valoir à son encontre. En effet, dans le contexte d'un système de surveillance comme Echelon, il ne paraît guère raisonnable, pour reprendre l'exemple du slovaque qui téléphone à un norvégien via des relais autrichiens et danois, d'exiger qu'il s'adresse aux instances de recours anglaises et/ou allemandes.

Il a été vu plus haut que l'adhésion à la Convention fait peser sur les Etats parties des obligations d'une force et d'une nature particulières, ce qui peut influencer le champ d'application spatial des mécanismes de mise

(346) Décision de recevabilité de la Commission du 10 juillet 1978, req. n° 8007/77, *Chypre c. Turquie*, §§ 33-34.

(347) En l'occurrence, des recours étaient bien institués mais le comportement du parquet turc, qui avait l'obligation d'enquêter sur l'espèce mais n'y procéda pas, pouvait légitimement faire nourrir au requérant un sentiment d'impuissance face à l'Etat. Voyez également dans l'arrêt *Aksoy c. Turquie* du 18 décembre 1996, son § 51 dans lequel la Cour, qui n'a d'ailleurs pas jugé nécessaire d'établir l'existence d'une pratique administrative, rappela de manière générale que *« la règle de l'épuisement des voies de recours internes (...) impose aux personnes désireuses d'intenter contre l'Etat une action devant un organe judiciaire ou arbitral international l'obligation d'utiliser auparavant les recours qu'offre le système juridique de leur pays »* (c'est nous qui soulignons).

(348) Il sera à cet égard très intéressant de voir comment le Tribunal de grande instance de Paris accueillera la plainte contre X déposée, à propos du programme Echelon, par l'association de défense d'utilisateurs d'Internet Akawa qui a préféré de la sorte opter pour l'épuisement des voies de recours françaises avant de s'adresser à la Cour européenne des droits de l'homme (*Le Figaro* 24.03.2000).

en œuvre de la responsabilité internationale des Etats tels que dégagés par la Commission du Droit International. Ces mécanismes communs comportent bien évidemment l'obligation d'épuiser au préalable les voies de recours internes qui reste le principe en droit des gens; ils peuvent être assouplis par l'adhésion à un instrument de protection des droits de l'homme.

71. Le parallèle avec le droit international de la mer — Dans son arrêt au fond, rendu le 1^{er} juillet 1999 dans l'affaire du *Saiga*, le Tribunal International du Droit de la Mer a accepté que les recours organisés par la Guinée ne devaient pas être épuisés par Saint Vincent et les Grenadines. Ce dernier pays se plaignait de ce que les douanes guinéennes avaient attaqué, blessant deux membres d'équipage, un pétrolier battant son pavillon à la limite de la zone économique exclusive guinéenne. Le Tribunal a estimé que la Guinée n'avait pas de titre international valable de « juridiction » pour agir de la sorte, ce qui entraînait la non-obligation d'épuiser ses voies de recours internes, les deux parties à l'instance ayant convenu qu'

« une condition préalable à l'application de la règle est qu'il doit exister un lien juridictionnel entre la personne ayant subi le préjudice et l'Etat responsable de l'acte illicite qui a causé le préjudice » (349).

Or, le Tribunal a estimé que l'application par la Guinée de sa législation douanière dans la zone économique exclusive relevant de sa compétence était contraire à l'article 60, § 2, de la Convention de Montego Bay qui limite cette application aux îles artificielles, installations et ouvrages y situés, sans quoi il y aurait une restriction aux droits des autres Etats dans ladite zone. Le Tribunal a tout autant rejeté le motif d'application extra-territoriale de la législation douanière qui reposait sur l'état de nécessité, faute pour la Guinée d'avoir démontré l'existence d'un péril grave et imminent pour ses intérêts essentiels et que cela aurait constitué le seul moyen d'éviter la violation de ces intérêts. Le Tribunal International du Droit de la Mer ayant conclu à l'illicéité d'une telle exécution extra-territoriale, poursuit en déclarant contraires à la Convention de Montego Bay l'arraisonnement et l'immobilisation du navire. C'est donc par l'analyse du fond du litige que cette juridiction internationale a fait échec à une exception d'irrecevabilité :

« le Tribunal conclut qu'il n'existait pas de lien juridictionnel entre la Guinée et les personnes physiques et morales au sujet desquelles Saint-Vincent-et-les-Grenadines a présenté des demandes. De ce fait, pour ce motif également, la règle qui requiert l'épuisement des recours internes ne s'applique pas à l'espèce » (350).

(349) Voyez le § 99 de l'arrêt du 1^{er} juillet 1999 du T.I.D.M. dans l'affaire du *Saiga* (n° 2), précitée.

(350) § 100 de l'arrêt *Saiga*, qui renvoie aux §§ 110 à 136 qui traitent en détail au fond la question de l'applicabilité extra-territoriale de la législation douanière.

Une telle solution est néanmoins contestée par des auteurs qui estiment que l'effectivité du rapport de sujétion en fait doit primer sur l'illégalité au regard du droit international de ce rapport, ce qui entraîne l'obligation d'épuiser les recours internes puisque celle-ci a pour but de permettre au souverain de remédier à l'illégalité (351).

Soutenir qu'un requérant qui ne se trouve pas valablement sous la « juridiction » d'un Etat partie à la Convention européenne des droits de l'homme n'aurait pas à épuiser les voies de recours organisées par cet Etat (même si il relève en fait de ladite « juridiction » vu l'existence de la violation de son droit au respect de la vie privée et de la correspondance qui le met en position de « victime » apte à la contester devant la Cour), est une thèse qui mérite certes d'être évoquée (352). Pour séduisante qu'elle soit, sachant que l'adhésion à la Convention peut emporter des dérogations au droit commun de la responsabilité internationale, cette thèse pâtit cependant de l'absence de précédent clairement et incontestablement applicable dans la jurisprudence strasbourgeoise.

Quoi qu'il en soit, d'autres motifs permettent de contester, dans les circonstances propres tenant à l'existence du programme Echelon, l'applicabilité de la règle de l'épuisement.

b. *L'absence d'« effectivité » et d'« accessibilité » des recours internes instaurés contre Echelon*

72. Quand le fond influence la forme et réciproquement — Un autre argument pour ne pas appliquer la règle de l'épuisement tient dans l'impossibilité pratique d'actionner les voies de recours nationales lesquelles peuvent difficilement passer pour « effectives ». En effet, vu la pluralité de pays potentiellement en cause, devant les juridictions ou instances de contrôle duquel agir ? Les Etats qui participent à Echelon ont-ils instauré des recours spécifiques, séparément, ensemble, ou encore internes à cette structure ? Et en admettant que les divers recours nationaux doivent être quand même épuisés, qu'advierait-il en cas de décisions nationales discordantes, par exemple si l'instance anglaise refuse l'accès aux données mémorisées qu'une instance d'un autre Etat participant mais non Partie à la Convention aurait de son côté accordé ? Ces recours existent-ils d'ailleurs ? Et sont-ils accessibles aux personnes ne vivant pas en Grande-Bretagne ou en Allemagne ?

La question de procédure posée par l'obligation d'épuiser en principe les voies de recours internes rejoint ici intimement le fond des violations alléguées. Il a été soutenu plus haut que l'absence d'une « loi » à la fois « acces-

(351) J. SALMON et E. DAVID, *Droit des gens*, t. II, *op. cit.*, p. 386.

(352) En effet, il faut se rappeler que le Gouvernement belge, notamment, invoque le droit international de la mer pour conférer un effet extra-territorial aux saisies informatiques.

sible » et « prévisible » déterminant la procédure d'élaboration et de contestation des écoutes et interceptions téléphoniques était de nature à violer l'article 8 de la Convention. Une telle absence de garanties procédurales peut aussi se révéler en contrariété avec l'exigence de « nécessité dans une société démocratique ». Ces manquements se répercutent inévitablement sur le droit à un recours effectif devant une instance nationale tel que garanti par l'article 13 de la Convention. Or, comme l'arrêt *Aksoy contre Turquie* l'a réaffirmé, l'article 13 présente d'étroites affinités avec la règle de l'épuisement préalable (353). Un défaut manifeste d'« effectivité » des recours nationaux pose dès lors problème tant au fond que sur le plan procédural et inversement (354); ce défaut découle ici, entre autres, du manque d'« accessibilité » des procédures censées être applicables dans le cadre d'Echelon.

Il est en outre probable que les Etats incriminés se réfugieraiient derrière des motifs de sécurité nationale ou l'immunité de juridiction des services de renseignement étrangers qu'ils accueillent sur leur territoire. Mais le fait que les gouvernements et les services de renseignement des Etats participants refusent de reconnaître l'existence ou non d'Echelon est de nature à conforter l'absence d'effectivité des hypothétiques recours que leurs droits internes respectifs comporteraient (355).

c. *Un programme de surveillance électronique globale constitue une « pratique administrative » dont l'existence dispense tout requérant d'épuiser au préalable les voies de recours internes*

73. Une jurisprudence surtout développée dans le cadre de requêtes interétatiques — L'existence d'un ensemble d'actes de contrainte à portée extra-territoriale, comme une écoute téléphonique ou toute autre interception de tout autre message, paraît présenter les caractéristiques d'une pratique administrative pour les personnes qui se trouvent sous la juridiction, valable elle, d'un autre Etat.

(353) Voyez également l'arrêt *Rotaru c. Roumanie* du 4 mai 2000, § 40, qui a renvoyé au fond à l'analyse de l'article 13 celle de l'exception préliminaire sur le non-épuisement des voies de recours internes dans une affaire de fichage per les services de renseignement.

(354) Pour un cas d'interaction entre l'article 8 et l'article 35 qui n'impose pas que soit actionné un recours voué à l'échec : Comm.eur.d.h., décision du 31 mars 1995, req. n° 18143/91, *A.G. c. France* (« <http://www.dhcour.coe.fr/Hudoc1doc/hfdec/sift/1151.txt> »). La Commission a estimé en l'espèce que la jurisprudence de la Cour de cassation française sur les écoutes au regard de l'article 8 n'accueillait que les pourvois dirigés contre des écoutes suscitées par stratagème ou dans des conditions obscures au mépris des droits de la défense, ce qui vouait à l'échec tout pourvoi invoquant un autre grief.

(355) Voyez les diverses déclarations recensées dans la partie I.A.1, en particulier celles des services américains et du Premier Ministre britannique. Dans une affaire où étaient allégués des mauvais traitements subis dans un commissariat de police, l'arrêt *Selmouni c. France* du 28 juillet 1999, § 76, considéra comme circonstance particulière de nature à dispenser de l'obligation d'épuiser les recours la passivité totale des autorités lorsqu'elles ne procèdent pas à l'ouverture d'une enquête ou si elles ne proposent aucune aide face à des allégations sérieuses selon lesquelles les agents de l'Etat auraient causé un dommage.

La notion de « pratique administrative » avait été au cœur de l'*Affaire Grecque*, traitée par la Commission suite aux requêtes des pays scandinaves et des Pays-Bas contre le régime des colonels (356). Certes, l'arrêt *Irlande contre Royaume-Uni* a bien rappelé que la règle de l'épuisement des voies de recours internes était valable pour les deux types de requêtes, étatiques et particulières, mais

« elle ne s'applique en principe pas [si l'État] attaque une pratique en elle-même, dans le but d'en empêcher la continuation ou le retour et sans inviter (...) la Cour à statuer sur chacun des cas qu'il cite à titre de preuves ou exemples de ces pratiques » (357).

C'est en cela que

« la notion de pratique offre un intérêt particulier pour le jeu de la règle de l'épuisement des voies de recours internes » (358).

Une étude doctrinale récente expose clairement que

« [l'exception à la règle de l'épuisement] prend naissance face à une pratique administrative qui rend toute procédure vaine ou inefficace, dans la mesure où cette pratique ne repose précisément sur aucun texte légal ou réglementaire qui donnerait une base formelle à un recours » (359).

L'ampleur sans précédent des violations alléguées commande de donner exception à la règle de l'épuisement. La jurisprudence de l'ancienne Commission européenne des droits de l'homme admettait déjà que l'existence d'une pratique administrative puisse être également invoquée par un ou plusieurs requérants particuliers (360).

74. La Cour admet désormais qu'un particulier puisse également se prévaloir de l'existence d'une « pratique administrative » — La Cour elle-même ne voit pas d'objection à ce qu'un ou des particuliers invoquent l'existence de pratiques administratives. Ainsi, dans l'affaire *Akdivar et autres contre Turquie*, a-t-elle constaté la violation concomitante des articles 8 (droit au respect du domicile) et 1^{er} du Premier Protocole (droit au respect des biens) du fait que les forces spéciales turques ont délibérément incendié les habitations des requérants dans le sud-est du pays alors que le Gouvernement turc se bornait à nier la participation de ses troupes

(356) Sur cet aspect particulier, la décision de recevabilité du 24 janvier 1968 dans l'*Affaire grecque*, *Ann.C.E.D.H.* 1968, p. 691.

(357) Arrêt *Irlande c. Royaume-Uni* du 18 janvier 1978, § 159.

(358) Arrêt *Irlande c. Royaume-Uni*, *ibidem*.

(359) D. DE BRUYN, « L'épuisement des voies de recours internes », in *La procédure devant la nouvelle Cour européenne des droits de l'homme après le Protocole n° 11*, Bruxelles, Nemesis et Bruylant, 1999, pp. 57-60.

(360) K. BOYLE et H. HANNUM, « Individual applications under the European convention on Human rights and the concept of administrative practice : the Donnelly case », *A.J.I.L.* 1974, pp. 440-453; A. CANCADO TRINDADE, *The application of the rule of exhaustion of local remedies in international law — Its rationale in the international protection of individual rights*, Cambridge University Press, 1983, pp. 193-211.

et n'avait avancé aucun élément de nature à justifier de telles ingérences. Après le constat de violation, la Cour a encore affirmé que

« les éléments recueillis par la Commission ne lui permettent pas de conclure dans un sens ou un autre sur l'allégation d'existence d'une pratique administrative contraire à ces articles » (361).

Autrement dit, elle ne dénie pas aux requérants individuels la possibilité d'invoquer, tant au fond — puisqu'il s'agit là d'éléments de fait — qu'au plan procédural, l'existence de telles pratiques. De surcroît, l'affaire n'avait pas trait à l'article 3 de la Convention prohibant la torture et les traitements inhumains et dégradants qui avait jusqu'à présent presque seul alimenté le contentieux sur les pratiques administratives.

Dans le même arrêt *Akdivar*, la Cour a d'ailleurs synthétisé sa jurisprudence relative à l'épuisement des voies de recours internes sans faire de distinction selon la qualité individuelle ou étatique de la partie requérante :

« (...) rien n'impose d'user des recours qui ne sont ni adéquats ni effectifs. De plus, selon les 'principes de droit international généralement reconnus', certaines circonstances particulières peuvent dispenser le requérant de l'obligation d'épuiser les recours internes qui s'offrent à lui (arrêt Van Oosterwijk c. Belgique du 6 novembre 1980, série A n° 40, pp 18-19, §§ 36-40). Cette règle ne s'applique pas non plus lorsqu'est prouvée l'existence d'une pratique administrative consistant en la répétition d'actes interdits par la Convention et la tolérance de l'Etat, de sorte que toute procédure serait vaine ou ineffective (arrêt Irlande c. Royaume-Uni du 18 janvier 1978, série A n° 25, p 164, § 159, et rapport de la Commission dans cette même affaire, série B n° 23-I, pp 394-397) » (362).

La Cour interaméricaine des droits de l'homme admet également des exceptions de cette nature au principe de l'épuisement des voies de recours internes (363).

75. Echelon rassemble toutes les caractéristiques de « pratiques administratives » — L'existence d'une « pratique administrative » relève donc également les éventuels requérants particuliers de l'obligation d'épuiser les voies de recours internes qui seraient organisées par les Etats participant au programme Echelon. La définition de la « pratique administrative » arrêtée dans l'affaire *Irlande contre Royaume Uni* est sans équivoque :

« une pratique incompatible avec la Convention consiste en une accumulation de manquements de nature identique ou analogue assez nombreux et liés entre eux pour ne pas se ramener à des incidents isolés ou à des exceptions, et pour former un ensemble ou un système » (364).

(361) Arrêt *Akdivar et autres c. Turquie* du 16 septembre 1996, § 88.

(362) Arrêt *Akdivar et autres c. Turquie*, § 67.

(363) Cour interam.d.h., avis consultatif du 10 août 1990 sur *Les exceptions à l'épuisement des recours internes*, Série A, n° 11.

(364) Arrêt *Irlande c. Royaume Uni* du 18 janvier 1978, § 159.

Les conditions de l'existence d'une pratique administrative ont été résumées par le professeur Picard (365). Il s'agit de :

- 1) « *la gravité de la violation de la Convention par les faits litigieux, cette gravité résultant autant du caractère flagrant de la violation que de l'éminence des droits violés* » ; vu les mots très sévères de la jurisprudence constante de la Cour européenne des droits de l'homme, depuis l'arrêt *Klass* en 1978 (qui voit dans la surveillance secrète des citoyens une caractéristique de l'Etat policier) jusqu'aux trois arrêts *Amann*, *Rotaru* et *Khan* rendus au cours du premier semestre 2000, l'éminence des droits violés ne fait aucun doute ; l'émoi provoqué par l'existence d'Echelon dans les enceintes parlementaires nationales d'Europe et d'Amérique ainsi qu'au Parlement européen ne laisse non plus guère de place au doute quant à son existence et au caractère flagrant des violations qu'il emporte ;
- 2) « *la répétition des violations* » ; la Cour estime que toute écoute est en soi une ingérence qui ne peut être validée que si chacune des écoutes de particuliers pris séparément répond aux trois exigences cumulatives de légalité, de légitimité et de nécessité ; et le programme Echelon est en lui-même « *un ensemble ou un système* » ;
- 3) « *la tolérance de ces faits par l'Etat défendeur ; celle-ci résulte elle-même de l'absence de réactions significatives de la part des autorités de l'Etat pour tenter sérieusement d'y mettre fin ; (...) il semble que l'existence même de ces pratiques, dès lors qu'elles sont suffisamment répandues, peut laisser présumer la tolérance, les gouvernements n'étant pas recevables à plaider ni l'ignorance des faits ni l'impuissance à y mettre fin* » ; la déclaration du Premier Ministre Britannique qui s'est borné à affirmer que le Royaume Uni ne profitait pas du programme Echelon pour espionner ses partenaires de l'Union Européenne est pour le moins laconique : ne porte-t-elle pas confirmation implicite de ce que ce programme existe bel et bien et de ce que cet Etat n'a encore rien entrepris pour y mettre un terme (366) ?

La dénonciation d'Echelon à l'aide de la jurisprudence sur les pratiques administratives coïncide avec un mouvement d'interprétation des techniques de contrôle par la Cour européenne des droits de l'homme nettement plus favorable que par le passé pour les victimes de violations structurelles ; la neutralisation plus régulière de la règle de l'épuisement des voies de

(365) E. PICARD, « Article 26 », *op. cit.*, p. 809.

(366) Le Premier Ministre britannique a affirmé que « *non, le Royaume Uni n'a pas trahi ses partenaires européens en collaborant étroitement avec les Etats Unis* » (*La Libre Belgique* 24.02.2000 ; aussi *Le Monde* 25.02.2000). Sur la portée des déclarations des plus hautes autorités d'un Etat qui engagent celui-ci en droit international : C.P.J.I., *Affaire du Groenland Oriental*, Série A, n° 53, p. 71.

recours interne et, en particulier, une attitude plus favorable quant à l'admission des pratiques administratives en attestent (367).

b) *L'obligation d'introduire la requête dans le délai de six mois à dater de la décision interne définitive n'est pas requise non plus*

76. Le cas des violations « continues » de la Convention — Il y a étroite corrélation entre la condition de l'épuisement préalable et le délai de six mois tous deux portés par l'article 35 de la Convention (368). L'allégation de l'existence d'une « pratique administrative » pouvant mener à ce que les recours internes ne doivent pas être épuisés, de même que les autres motifs évoqués plus haut à cet égard, l'absence de recours à épuiser relève forcément de l'obligation de respecter ce délai. Les principes du droit international recommandent toutefois d'introduire les recours dans des délais raisonnables (369).

Qui plus est, il peut aussi être soutenu que la situation en contrariété avec la Convention est persistante. Ainsi, dans une affaire *Chypre contre Turquie* précitée, l'ancienne Commission européenne des droits de l'homme a tenu à confirmer avec force sa propre jurisprudence selon laquelle

« lorsqu'il existe 'une situation qui dure encore', la question de la règle des six mois ne pourra se poser que lorsque la situation aura cessé » (370),

à plus forte raison quand n'existe aucun recours (371). En effet, tant que le programme Echelon existe dans l'état arbitraire qui est supposé le sien, à savoir tant qu'il continuerait à permettre l'interception des communications continentales, il y a lieu de considérer qu'

« il faut (...) que la violation de la Convention cesse pour que le droit d'action tendant à la condamner devienne prescriptible » (372).

2. Les conditions propres aux requêtes individuelles devant la Cour : la notion de « victime potentielle » en cas d'atteintes secrètes aux droits fondamentaux

77. Un particulier ne peut contester une « loi » ou une « pratique administrative » *in abstracto*... — Dans les conditions prévues par l'ar-

(367) Cons. à nouveau J.F. FLAUS, « La Cour de Strasbourg face aux violations systématiques des droits de l'homme », *op. cit.*, pp. 353-361.

(368) Comm.eur.d.h., décision du 9 juin 1958, req. n° 214/56, *De Becker c. Belgique*, Ann. C.E.D.H. 1958, p. 215.

(369) E. PICARD, « Article 26 », *op. cit.*, p. 610 et la jurisprudence citée. L'établissement du rapport définitif du Parlement européen sur Echelon constituerait une balise non négligeable pour le comput de ce délai raisonnable.

(370) Décision de recevabilité précitée sur la requête n° 8077/77, § 44.

(371) Comm.eur.d.h., décision du 9 décembre 1987, req. n° 11123/84, *Tête c. France*, D.R. 54, p. 53.

(372) M. KAISER et P. LAMBERT, « Le délai de six mois », in *La procédure devant la nouvelle Cour européenne des droits de l'homme après le Protocole n° 11*, Bruxelles, Nemesis et Bruylant, 1999, p. 70.

ticle 35, § 2, de la Convention (373), l'article 34 autorise toute personne physique, toute organisation non gouvernementale ou tout groupe de particuliers à présenter une requête à la Cour européenne des droits de l'homme. Les particuliers rencontrent cependant cette difficulté supplémentaire, si l'on compare leur situation à celle des États, qu'ils doivent prouver avoir été « victimes » au sens de son article 34 d'une violation de la Convention (374).

La jurisprudence européenne continue à refuser l'*actio popularis* (375). Ceci semble confiner dans l'irrecevabilité les requêtes introduites par les associations pour défendre un intérêt collectif (376). Les personnes morales peuvent toutefois introduire une requête pour peu qu'elles justifient être elles-mêmes victimes d'une violation de l'article 8, ce qui implique que les droits garantis soient compatibles avec la nature de telles personnes (377).

(373) La requête individuelle ne peut être anonyme, avoir déjà été soumise à un autre organisme international, incompatible avec la Convention, ni manifestement mal fondée, ni abusive. Ces autres conditions ne sont pas analysées plus avant dans la mesure où la condition la plupart du temps non remplie est celle de l'apparence de fondement, apparence étant pour sa part justement analysée tout au long du présent article.

(374) Cf. par exemple la décision de la Commission sur la requête n° 299/57, *Ann. CEDH*, 1958, p. 191 : l'État n'est pas astreint à fournir un commencement de preuve au stade de la recevabilité, pareille recherche touchant au fond de l'affaire. Il aurait par ailleurs été intéressant, en raison du caractère international d'une affaire d'entraide judiciaire, que la nouvelle Cour examine si pouvait se prétendre « victime », au sens de l'article 34, le requérant qui contestait le séquestre en Suisse et la transmission aux autorités belges de documents d'une personne le concernant qui avaient été saisis dans les mains d'une tierce personne sur la base d'une ordonnance notifiée à cette dernière. L'article 8 n'ayant manifestement pas été violé, en l'espèce, la décision d'irrecevabilité de la Cour du 15 décembre 1998, req. n° 27819/95, *Vercambre c. Suisse* (inédite) n'a toutefois pas procédé à l'examen de la qualité de victime.

(375) En dernier lieu, l'arrêt *Ihan c. Turquie* du 27 juin 2000, §§ 51 et suiv. qui admet toutefois qu'un parent introduise une requête à la place d'une personne en situation de « vulnérabilité ».

(376) Comm.eur.d.h., décision d'irrecevabilité du 16 avril 1991, req. n° 15404/89, *Purcell et autres c. Irlande*, D.R. 70, p. 262 qui considère que le requérant doit montrer que les mesures dont il se plaint ont été appliquées à son détriment et qu'il en a subi directement les effets. Un syndicat, une organisation non gouvernementale n'ont pas qualité, faute de pouvoir se prétendre eux-mêmes victimes, pour introduire une requête dirigée contre une mesure qui frappe leurs membres. A ce sujet : L.E. PETTITI et O. DE SCHUTTER, « Le rôle des associations dans le cadre de la Convention européenne des droits de l'homme », *J.T.D.E.* 1996, pp. 145-150.

(377) Comm.eur.d.h., décision d'irrecevabilité du 14 janvier 1998, req. n° 32200/96 et n° 32201/96, *Herbecq et association « Ligue des droits de l'homme » c. Belgique*, *Ann. CEDH*, vol. 41, 1998, p. 63, a refusé de reconnaître la qualité de victime à une association contestant, sur base de l'article 8, l'absence de législation sur les systèmes de surveillance dans les lieux publics au motif qu'une personne morale ne peut être filmée et ne peut donc pas être atteinte par l'utilisation d'appareils de prise de vues. Il est vrai aussi que le droit communautaire applicable aux bases de données ne protège que très partiellement les personnes morales. Il devrait toutefois en aller différemment en cas d'écoutes téléphoniques, en tout cas lorsqu'elles aboutissent au stockage informatique de données sur la politique commerciale des entreprises, en particulier si une entreprise perd un marché parce qu'une concurrente aurait été informée de ses intentions par des services de renseignement. Un tel raisonnement pourrait aussi être, par exemple, tenu à propos de la collecte de renseignements sur les partis politiques. Le droit communautaire devrait cependant évoluer dans le sens de la permission de l'invocation des Directives « vie privée » par les personnes morales dans les cas ici évoqués (cf. l'article 1^{er}, § 2, de la proposition présentée de la Commission, COM(2000) 385, p. 16).

Les particuliers ne rencontrent pas cet obstacle, ce qui ne les dispense pas de prouver avoir été « victimes ».

Le risque d'ingérence et de violation des droits au respect de la vie privée et de la correspondance qui est encouru par tout un chacun, par cela seul qu'il est usager des services publics ou privés de télécommunications, est inconnu. Mais il est réel puisque, à en croire les rapports en cours d'examen au Parlement européen, des millions de conversations téléphoniques et autres messages pourraient être interceptés et surveillés chaque jour selon des critères impossibles à déterminer. Le danger semble présent même s'il est difficile à circonscrire (ce qui est d'ailleurs le problème).

La contestation des effets qu'une « loi » ou une « pratique administrative » peut entraîner par sa seule existence est néanmoins parfaitement possible dès lors que cette loi ou cette pratique n'est pas contestée *in abstracto* mais bien parce que ses effets potentiels, même en l'absence d'application effective, sont de nature à violer la Convention (378).

78. ... à moins qu'il ne prouve qu'il est « potentiellement » la victime de ses effets, ce que la Cour a admis dès 1978 en matière d'écoutes téléphoniques — C'est à nouveau dans l'arrêt *Klass contre Allemagne* qu'une notion aussi importante que celle de « victime potentielle » a été dégagée. Et précisément dans une affaire d'écoutes téléphoniques. La notion n'est pas pour autant limitée à ce genre de contentieux (379). La Cour en avait déjà fait application en ayant à s'interroger sur l'influence que l'existence même d'une législation en matière d'enseignement pouvait avoir sur les droits garantis par le 1^{er} Protocole additionnel (380). La Cour l'applique également à propos des législations nationales incriminant l'homosexualité (381).

L'arrêt *Klass* a commencé par rappeler la différence existant entre requête interétatique et requête individuelle. La nature particulière, exposée plus haut, des obligations objectives souscrites par les Etats ont pour contrepartie l'absence de justification d'un intérêt à agir dans leur chef, de telle manière qu'ils peuvent contester une législation tierce en soi. Par contre,

(378) La jurisprudence du C.D.H. va dans le même sens du refus du contrôle *in abstracto* : décision du 3 avril 1997, com. n° 558/1993, *Canepa c. Canada*, point 6.3.

(379) Pour un point récent, voyez G. COHEN-JONATHAN, *Aspects européens des droits fondamentaux*, 2^e éd., Paris, Montchrestien, 1999, pp. 28-29 : « la Commission et la Cour ont en effet admis dans certains hypothèses qu'un individu pouvait se prétendre victime au sens de l'article 25 (actuel article 34), du seul fait de l'existence d'une législation contraire à la Convention dont il risquait spécialement de subir les effets et ceci indépendamment de toute application effective ». Également P. LAMBERT, « Les bénéficiaires du droit de recours », in *La procédure devant la nouvelle Cour européenne des droits de l'homme après le Protocole n° 11*, Bruxelles, Nemesis et Bruylant, 1999, pp. 16-19.

(380) Arrêt *Affaire linguistique belge* du 23 juillet 1968 et arrêt *Kjeldsen, Busk Madsen et Pedersen* du 7 décembre 1976, § 48.

(381) La première fois dans l'arrêt *Dudgeon c. Royaume Uni* du 22 octobre 1981, § 41.

« [l'article 34] n'institue pas au profit des particuliers une sorte d'actio popularis pour l'interprétation de la Convention; il ne les autorise pas à se plaindre in abstracto d'une loi par cela seul qu'elle leur semble enfreindre la Convention. En principe, il ne suffit pas à un individu requérant de soutenir qu'une loi viole par sa simple existence les droits dont il jouit aux termes de la Convention; elle doit avoir été appliquée à son détriment. Néanmoins (...), elle peut violer par elle-même les droits d'un individu s'il en subit directement les effets, en l'absence de mesure spécifique d'exécution » (382).

La Cour poursuit en posant que le caractère secret de la violation alléguée ne saurait faire obstacle à

« l'effet utile de la Convention [qui] implique, en pareilles circonstances, une possibilité d'accès à la Commission ».

Aussi,

« la Cour accepte donc qu'un individu puisse, sous certaines conditions, se prétendre victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation en permettant, sans avoir besoin d'avancer qu'on les lui a réellement appliquées » (383).

La Cour s'est prononcée dans le même sens à propos du système du comptage des conversations téléphoniques dès lors que le requérant se range dans une catégorie de personnes risquant de tomber sous le coup d'une telle pratique, indépendamment même de toute mesure d'application concrète à son égard (384).

Les motifs qui ont conduit la Cour européenne des droits de l'homme à confirmé la recevabilité de la requête dans l'affaire *Klass* sont particulièrement pertinents dans le cas d'Echelon :

« la législation incriminée institue un système de surveillance exposant chacun, en République fédérale d'Allemagne, au contrôle de sa correspondance, de ses envois postaux et de ses télécommunications, sans qu'il le sache jamais à moins d'une indiscretion ou d'une notification ultérieure (...). Ladite législation frappe par là directement tout usager ou tout usager virtuel des services des postes et télécommunications de la R.F.A.. En outre (...), on peut dénoncer cette menace de surveillance comme restreignant par elle-même la liberté de communiquer au moyen de ces services et comme constituant donc, pour chaque usager ou usager virtuel, une atteinte directe au droit garanti par l'article 8 » (385).

La Cour a enfin précisé que l'indication rétrospective par les autorités allemandes qu'aucune mesure de surveillance secrète n'avait été ordonnée

(382) Arrêt *Klass c. Allemagne* du 4 juillet 1978, § 33. L'arrêt *Amann c. Suisse* du 16 février 2000 a également rappelé, dans le cadre de l'article 13 qui porte le droit à un recours effectif devant une instance nationale, que « dans une affaire issue d'une requête individuelle, [la Cour] n'a pas pour tâche de contrôler dans l'abstrait une législation ou une pratique contestée, mais doit autant que possible se limiter, sans oublier le contexte général, à trilater les questions soulevées par le cas concret dont elle se trouve saisie » (§ 88).

(383) Arrêt *Klass*, § 34. La qualité de victime peut en effet exister en l'absence de préjudice (arrêt *Ihlan c. Turquie* du 27 juin 2000, § 52).

(384) Arrêt *Malone c. Royaume Uni* du 27 juin 1984, § 86.

(385) Arrêt *Klass*, § 37. C'est nous qui soulignons.

ou exécutée à l'encontre des requérants était sans incidence sur l'appréciation de leur qualité de victime (386). Dans un environnement désormais libéralisé comme celui des télécommunications, les conclusions de la Cour restent évidemment d'actualité.

Cette jurisprudence permettant de contester directement une législation dont un individu risque de subir les effets en contrariété avec les droits fondamentaux qui lui sont reconnus dans un instrument international n'est pas isolée. Le Comité des droits de l'homme de l'O.N.U. (387). et la Cour interaméricaine des droits de l'homme se sont également prononcés en ce sens (388). Ainsi que l'a souligné en 1999 le rapporteur spécial sur la responsabilité internationale des Etats devant la Commission du Droit International de l'O.N.U.,

« les divers organes compétents en matière de droits de l'homme ont une attitude très semblable à l'égard du problème. La législation peut, en soi, constituer une violation de la convention concernée, si elle est directement applicable aux particuliers ou que son application les menace directement, encore que la question de savoir si elle la viole dans un cas donné est subordonnée à un examen des faits de l'espèce. Des recours internes peuvent peut-être permettre d'obtenir réparation, mais ils ne sauraient en tenir lieu » (389).

Cette dernière appréciation a été en tous points confirmée le 4 mai 2000 par l'arrêt *Rotaru contre Roumanie* qui reconnut la qualité de victime à une personne fichée par les services de renseignements (en raison de la seule existence de mesures secrètes ou d'une législation les permettant) et indiqua aussi qu'une décision favorable ultérieure ne retire la qualité de victime que si les autorités nationales ont reconnu puis réparé la violation (390).

79. Un commencement « raisonnable » de preuve peut difficilement être exigé face à un programme international et secret — Se pose certes, dans le chef des requérants individuels voulant contester Echelon, le problème du commencement raisonnable de preuve d'une ingérence

(386) M. MELCHIOR, « La procédure devant la Commission européenne des droits de l'homme », in *Introduire un recours à Strasbourg ? — Een zaak aanhangig maken te Straatsburg?*, Bruxelles, Nemesis, 1986, p. 20, à propos de la notion de « victime potentielle » : « il s'agit en effet d'une situation où, en raison même de la nature des choses, il est impossible pour un requérant de savoir si la pratique qu'il estime contraire à la Convention lui a été effectivement appliquée ».

(387) C.D.H., décision du 31 mars 1993, com. n° 385/1989, *Mac Intyre c. Canada*, R.U.D.H., 1993, p. 156, point 10.4. et la jurisprudence citée par F. SUDRE, *Droit international et européen des droits de l'homme*, op. cit., pp. 430-431. Le C.D.H. demande également que les actes querellés aient déjà eu des conséquences négatives ou qu'il existe une menace réelle de telles conséquences (décision du 22 juillet 1996, com. n° 645/1995, *Bordes et Temaharo c. France*, point 5.4; décision du 20 octobre 1998, com. n° 646/1995, *Lindon c. Australie*, point 6.8).

(388) Cour interam. d.h., avis consultatif du 9 décembre 1994 sur *La responsabilité internationale pour la promulgation et l'exécution de lois en violation de la Convention*, Série A, n° 14, §§ 42 à 50.

(389) J. CRAWFORD, *Deuxième rapport sur la responsabilité internationale des Etats*, présenté lors de la 51^e session de la C.D.I., A/CN.4/498, p. 36.

(390) Arrêt *Rotaru c. Roumanie* du 4 mai 2000, § 35 et les renvois à la jurisprudence de la Cour, en particulier le § 34 de l'arrêt *Klass*.

secrète dans leur droit au respect de la vie privée. La Commission a à plusieurs reprises indiqué dans des affaires anglaises où étaient en cause le *Security Service Act* de 1989 que

« les requérants n'ont pas à apporter la preuve de l'allégation selon laquelle le Security Service continue à tenir un fichier comportant des informations personnelles sur eux » (391).

Toutefois, certains éléments cités en introduction, et à plus forte raison les pièces officielles des débats et questions soulevés dans différents parlements nationaux, sont de nature à étayer utilement les requêtes. Ceux-ci seront d'autant plus renforcés lorsque la commission temporaire instituée le 5 juillet 2000 par le Parlement européen aura établi son rapport.

Les requérants éventuels ont tout intérêt à contester l'existence même de lois et pratiques de surveillances secrètes contraires à la Convention en ce qu'ils peuvent en subir les effets plutôt que d'affirmer en avoir effectivement subies. Dans l'affaire *Halford*, la Cour conclut à la violation de l'article 8 pour des écoutes sur le téléphone professionnel mais conclut à l'absence de violation par des écoutes effectuées sur le téléphone du domicile. Comme la requérante ne contestait pas l'existence de la législation mais affirmait par contre avoir été l'objet d'écoutes effectives, elle devait alors apporter la preuve, avec une probabilité raisonnable, que de telles écoutes avaient eu lieu. N'ayant pu apporter cette preuve de l'ingérence, l'article 8 n'était pas violé (392). On se doute que pour le commun des mortels qui pourrait faire l'objet de surveillances dans le cadre du programme Echelon, l'apport d'une telle preuve tient de l'impossible.

3. Pourquoi aller à Strasbourg plutôt qu'à Genève ?

80. C'est dès lors l'extraordinaire cohérence de la jurisprudence strasbourgeoise, fruit de cinquante années de développements, qui doit mener les particuliers à préférer la requête devant la Cour européenne des droits de l'homme plutôt que la communication devant le Comité des droits de l'homme de l'O.N.U. Et ce d'autant plus que certains Etats protagonistes essentiels d'Echelon, comme les Etats Unis et le Royaume Uni, n'ont de toute façon pas souscrit au Protocole facultatif au Pacte international rela-

(391) Par exemple : Comm.eur.d.h., décision du 1^{er} septembre 1993, req. n° 20317/92, *Hewitt et Harman c. Royaume Uni*, trad. propre, « <http://www.dhcour.coe.fr/Hudoc1doc/hedec/sift/1472.txt> », p. 9 sur 13 qui poursuit que « *an applicant however cannot be reasonably expected to prove that information concerning his private life has been compiled and retained. It is sufficient, in the area of secret measures, that the existence of practices permitting secret surveillance be established and that there is a reasonable likelihood that the Security Service has compiled and retained information concerning his private life* ». Egalement la décision du 2 avril 1993, req. n° 18601/91, *Esbester c. Royaume Uni*, « <http://www.dhcour.coe.fr/Hudoc1doc/hedec/sift/1351.txt> », p. 8 sur 11. Et plus récemment la décision du 16 octobre 1996, req. n° 28756/95, *Matthews c. Royaume Uni*, « <http://www.dhcour.coe.fr/Hudoc1doc/hedec/sift/3181.txt> », p. 7 sur 10.

(392) Arrêt *Halford c. Royaume Uni* du 25 juin 1997, §§ 57 à 60.

tif aux droits civils et politiques permettant la saisine du Comité par des particuliers (II.B.3.).

81. Malgré les importantes similitudes existant entre la Convention et le Pacte international relatif aux droits civils et politiques, l'effectivité du système européen est plus grande — L'article 2, § 1^{er}, du Pacte international relatif aux droits civils et politiques du 16 décembre 1966 comporte une disposition largement semblable à l'article 1^{er} de la Convention concernant la reconnaissance de la jouissance des droits et libertés à toutes les personnes sous la juridiction de l'Etat partie (393). Le droit à la protection de la vie privée est garanti tant par l'article 8 de la Convention européenne des droits de l'homme que par l'article 17 du Pacte international relatif aux droits civils et politiques (394). Le droit à un recours effectif garanti par l'article 13 de la Convention trouve quant à lui son pendant dans l'article 2, § 3, du Pacte (395).

Les droits garantis paraissent *a priori* relativement semblables. Toutefois de notables différences existent entre le système européen et le système onusien (396).

La première tient au volume des affaires traitées. Le Comité des Droits de l'Homme a à connaître d'un contentieux nettement moins important en raison de facteurs qu'il ne convient pas d'exposer ici. En découle cependant la conséquence que sa jurisprudence est moins riche de cas d'applications.

Par ailleurs, le C.D.H. ne reconnaît le bénéfice des droits garantis par le Pacte qu'aux personnes physiques et non aux personnes morales ou groupements de fait, qu'il s'agisse de sociétés commerciales, d'associations ou d'organisations non-gouvernementales. La divergence avec le système européen est patente (397).

(393) Article 2, § 1^{er}, du Pacte : « Les Etats parties (...) s'engagent à respecter et à garantir à tous les individus se trouvant sur leur territoire et relevant de leur compétence les droits reconnus dans le présent Pacte, sans distinction aucune (...) ».

(394) Article 17 du Pacte : « 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation; 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». Voyez *supra* l'observation générale n° 16 du Comité des droits de l'homme.

(395) Article 2, § 3, du Pacte : « Les Etats parties au présent Pacte s'engagent à : a) garantir que toute personne dont les droits et libertés reconnus dans le présent Pacte auront été violés disposera d'un recours utile, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles; b) garantir que l'autorité compétente, judiciaire, administrative ou législative, ou toute autre autorité compétente selon la législation de l'Etat, statuera sur les droits de la personne qui forme le recours et développer les possibilités de recours juridictionnel; c) garantir la bonne suite donnée par les autorités compétentes à tout recours qui aura été reconnu justifié ».

(396) Pour une comparaison générale, cons. entre autres A.H. ROBERTSON et J.G. MERRILLS, *Human rights in the world — An introduction to the study of the international protection of human rights*, 4^e éd., Manchester University Press, 1996, pp. 54-72.

(397) L'article 2, § 1^{er}, du Pacte ne parle que d'« individus » là où l'article 34 ouvre les recours strasbourgeois à « toute personne physique, toute organisation non gouvernementale ou tout groupe ».

82. Le problème tenant aux degrés divers d'engagement en matière de droits de l'homme des Etats participant à Echelon — Il suffit de jeter un œil sur l'état des adhésions au Protocole facultatif autorisant l'introduction de communications individuelles auprès du Comité pour se rendre compte que des protagonistes essentiels du programme Echelon, comme le Royaume Uni et les Etats-Unis n'y sont pas parties, de même que le Japon qui accueillerait une station d'écoute. Les seuls pays parties prenantes au programme à avoir souscrit au Protocole sont l'Allemagne (25.08.1993), l'Australie (25.09.1991), le Canada (19.06.1976) et la Nouvelle-Zélande (26.05.1989) (398). L'Allemagne, qui est également partie à la Convention européenne des droits de l'homme, a émis une réserve sur le Protocole qui dispose que le Comité des droits de l'homme ne peut connaître d'une communication qui aurait déjà été traitée dans le cadre d'une autre procédure d'investigation ou de règlement international, ni d'une communication relative à une violation du Pacte qui trouverait son origine dans des faits antérieurs à l'entrée en vigueur du Protocole.

Dès lors, si une personne qui réside sur le territoire d'un Etat partie à la Convention désire contester le comportement du Royaume Uni, elle ne peut de toute façon que s'adresser à la Cour européenne des droits de l'homme. Si un requérant souhaite contester le comportement de l'Allemagne, il a le choix entre le système onusien et le système européen, lequel offre toutefois certainement les garanties analysées plus haut quant à l'imputabilité, à la jurisprudence de fond sur les écoutes téléphoniques et des principes clairs sur les conditions de recevabilité.

Une des raisons essentielles pouvant justifier le choix du système européen réside donc dans l'effectivité qui s'attache aux décisions et arrêts rendus à Strasbourg, effectivité nettement plus contraignante pour les Etats que celle du système onusien. Ceci sans remettre en cause la qualité de la jurisprudence du Comité mais en sachant que celui-ci évolue dans un cadre plus restrictif (399).

Le seul recours susceptible d'attirer un nombre significatif d'Etats collaborant au programme Echelon serait la communication qu'introduirait un

de particuliers ». S. MARCUS HELMONS, « L'applicabilité de la Convention européenne des droits de l'homme aux personnes morales », *J.T.D.E.* 1996, p. 151, note 8, recense bon nombre d'arrêts de la Cour rendus sur requête de personnes morales.

(398) L'état des ratifications au Pacte et à son premier Protocole facultatif, des déclarations d'acceptation des communications interétatiques sur base de l'article 41 du Pacte ainsi que les réserves et objections sur ces deux instruments date du 30.06.2000 quand a été consulté le site Internet de l'O.N.U. à l'adresse « <http://www.un.org/Depts/Treaty/final/ts2/newfiles/part-boo/iv-boo/iv-4.html> ».

(399) S. PARMENTIER, « Les mécanismes du respect des droits fondamentaux et leur importance pour la Belgique », in *50^e anniversaire de la Déclaration universelle des droits de l'homme*, colloque du 28 octobre 1998 organisé par les Ministères des Affaires étrangères et de la Justice, Bruxelles, Ministère des Affaires étrangères, 1999, p. 39.

Etat sur base de l'article 41 du Pacte (400). En effet, à l'exception du Japon, tous les pays directement parties à l'accord UKUSA ainsi que l'Allemagne ont déposé la déclaration d'acceptation des communications interrétatiques (401). Aucune n'a toutefois été introduite à ce jour. Cette absence de jurisprudence sur les communications étatiques ne permet pas de savoir *a priori* si le Comité accepterait qu'un Etat conteste en soi une législation ou une pratique en vigueur dans un ou plusieurs autres Etats, ce qui a son importance pour la règle de l'épuisement des voies de recours internes.

Faute de précédents significatifs, en-dehors de l'observation générale du C.D.H. sur l'article 17 du Pacte, il n'est pas sûr non plus que, l'Etat, comme le particulier, qui soumettrait une communication obtiendrait gain de cause quant au fond (402).

83. Alors que l'inverse n'est pas vrai, le Comité des Droits de l'homme accepterait peut-être plus facilement les communications déjà partiellement déferées à la Cour européenne des droits de l'homme — Paradoxalement peut-être, le plus grand libéralisme dont fait parfois preuve le Comité des droits de l'homme en ce qui concerne les conditions de recevabilité plaide également pour n'actionner le mécanisme des communications individuelles qu'en second lieu. L'exigence du délai de six mois pour introduire une requête, si importante dans le cadre de la Convention européenne des droits de l'homme, n'existe pas dans le Pacte (403).

Les organes de la Convention européenne des droits de l'homme refusent sur base de son article 35, § 2, b), la recevabilité des requêtes qui ont déjà

(400) Nous ne nous prononçons pas ici sur l'éventualité d'un recours étatique devant la Cour Internationale de Justice. Les déclarations facultatives d'acceptation de sa juridiction obligatoire n'ont été déposées que par l'Australie (17.02.1975), le Canada (10.05.1994 sous condition de réciprocité), le Japon (15.09.1958), la Nouvelle Zélande (22.09.1977 sous condition de réciprocité) et le Royaume Uni (01.01.1969 sous condition de réciprocité), à chaque fois sans préjudice d'un accord entre les éventuelles parties à l'instance pour soumettre le différend à un autre mode de règlement pacifique (site de la C.I.J. : « <http://www.icj-cij.org/cijwww/cdocumentbase/cbasicedeclarations.htm> »). L'Allemagne et, surtout les Etats Unis (qui ont fait défaut au fond dans l'*Affaire des Activités militaires et paramilitaires au Nicaragua*), ne paraîtraient à l'instance que sur base volontaire.

(401) L'Allemagne a remis la déclaration sur l'article 41 du Pacte le 22 janvier 1997. L'Australie, le Canada, la Nouvelle-Zélande, le Royaume Uni et les Etats Unis ont également déposé de telles déclarations.

(402) Deux difficultés majeures surgissent donc : le mécanisme de la communication étatique n'a jamais été actionné et la Grande-Bretagne comme les Etats Unis n'ont pas souscrit au Protocole facultatif sur les communications individuelles (voyez J. DHOMMEAUX, « Les Etats parties à la Convention européenne des droits de l'homme et le Comité des droits de l'homme de l'O.N.U. : de la cohabitation du système universel de protection des droits de l'homme avec le système européen », in *Liber Amicorum M.A. EISSEN*, Bruxelles et Paris, Bruylant et L.G.D.J., 1996, pp. 119 et 120).

(403) P. LAMBERT, « L'approbation du Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques », *J.T.* 1994, p. 610.

été portées devant le Comité (404). Le Comité quant à lui, est beaucoup plus accueillant.

Alors qu'aucune violation d'un droit n'a été constatée par la Commission européenne des droits de l'homme, le Comité a bien déclaré irrecevable la communication portant sur la même affaire, l'Etat défendeur ayant fait une réserve en ce sens (405). Il a toutefois déclaré irrecevable une communication en cours d'examen devant la Commission interaméricaine des droits de l'homme mais a indiqué qu'il pouvait reconsidérer sa décision si les motifs d'irrecevabilité devaient cesser d'exister (406). Et, malgré les réserves formulées à l'adhésion au Protocole facultatif par un Etat également partie à la Convention, il n'hésite pas à examiner le fond de requêtes déclarées irrecevables pour des questions de procédure à Strasbourg (407).

Le cas le plus célèbre de divergence entre Strasbourg et Genève est l'affaire *Casanovas contre France* dans laquelle la Commission européenne avait estimé que, faute d'entrer dans le champ d'application de l'article 6 de la Convention, les fonctionnaires ne bénéficiaient pas d'un procès équitable alors que, selon le Comité, l'article 14 du Pacte leur accordait le bénéfice d'un tel droit. La France avait pourtant formulé une réserve devant empêcher l'examen par le Comité d'une communication déjà examinée par la Commission européenne mais le Comité examina pourtant la demande et l'estima fondée (408).

Qu'il y ait ou non condamnation à Strasbourg, si l'on formule l'hypothèse que la Cour européenne serait préalablement saisie du cas Echelon, il faut tenir compte du jeu des adhésions, réserves et déclarations émises sur l'instrument européen et sur l'instrument universel. Dans le cas d'un recours introduit par un individu ressortissant à la juridiction d'un Etat par ailleurs partie à la Convention, il y aurait certes des différences, *ratione personae*, qui pourraient faire échec au principe « *non bis in idem* » puisque le nombre d'Etats contre lesquels serait dirigée la communication serait forcément différent, parce que ne peuvent être attraités devant la Cour euro-

(404) Comm.eur.d.h., décision d'irrecevabilité du 6 juillet 1992, req. n° 17512/90, *Calcerrada Fornelies et Cabeza Mato c. Espagne*, D.R. 73, p. 214. S. DEPRE, « Le principe 'non bis in idem' », in *Les exceptions préliminaires dans la Convention européenne des droits de l'homme*, Bruxelles, Nemesis et Bruylant, 1997, pp. 95-107.

(405) C.D.H., décision du 23 juillet 1999, com. n° 744/1997, *Urbanetz Linderholm c. Croatie*, point 4.2.

(406) C.D.H., décision du 25 mars 1999, com. n° 739/1997, *Tovar Acuña c. Venezuela*, points 5.2 et 6.b). Dans sa décision du 24 mars 2000, com. n° 824/1998, *Nicolov c. Bulgarie*, point 8.2, le Comité a posé que « ce n'est que lorsque la même question est déjà en cours d'examen devant une autre instance internationale d'enquête ou de règlement que le Comité n'est pas compétent ». Dans cette affaire où la Commission européenne des droits de l'homme avait pourtant déjà jugé la requête irrecevable, le Comité a donc écarté cette exception d'irrecevabilité.

(407) C.D.H., décision du 25 mars 1999, com. n° 716/1996, *Pauger c. Autriche*, point 6.4.

(408) Pour un exposé succinct de l'affaire *Casanovas* : C. SCIOTTI, *La concurrence des traités relatifs aux droits de l'homme devant le juge national*, Bruxelles, Nemesis et Bruylant, 1997, pp. 36-37.

péenne des droits de l'homme que les parties à celle-ci. L'Australie, la Nouvelle Zélande et le Canada pourraient être attirés devant le Comité. Mais pas l'Angleterre, ni les Etats Unis qui n'ont pas souscrit au Protocole facultatif sur les communications individuelles, l'Allemagne ayant de surcroît émis une réserve quant aux affaires déjà déferées à la Cour européenne.

Le recours le plus efficace serait donc celui qu'un Etat introduirait lui-même devant le Comité pour attirer tous les Etats participant à Echelon. Si l'Etat en question est Partie à la Convention européenne des droits de l'homme, il agirait cependant peut-être plus utilement en saisissant au préalable la Cour de Strasbourg. Parce que l'effectivité de la jurisprudence est plus grande; parce que l'affaire pourrait, le cas échéant, être quand même déferée ensuite devant le Comité en raison de la différence du nombre d'Etats potentiellement défendeurs; parce que, surtout, une requête interétatique pourrait utilement soutenir les requêtes que des particuliers introduiraient également auprès de la Cour européenne des droits de l'homme.

*

* *

84. Pour conclure : l'analyse d'Echelon offre en fin de compte l'occasion de rappeler tous les éléments qui constituent aujourd'hui l'« ordre public européen » — Tous les points de fond, d'imputabilité et de procédure développés dans la présente analyse du programme de surveillance électronique, globale et secrète, Echelon concernent peu ou prou l'ordre public européen.

L'ordre public européen a pour fondements le caractère objectif des obligations souscrites par les Etats Parties à la Convention laquelle est un système de garantie collective qui peut être mis en œuvre soit par les Etats qui disposent d'une « action publique », soit par les particuliers qui, à défaut de bénéficier d'une « *actio popularis* », peuvent, quelle que soit leur nationalité, prouver leur qualité de victime, même potentielle. Et ce en raison de l'atteinte au droit à l'intimité de la vie privée et au respect de la correspondance que constitue, pour eux, l'existence de la simple possibilité qu'il soit recouru à des mesures de surveillance secrète.

L'ordre public européen a pour contenu les valeurs communes patiemment dégagées par la jurisprudence strasbourgeoise et les droits constitutifs de la société démocratique.

Il a pour effets la pleine soumission de l'Etat au système de garantie collective de la Convention, ce qui rend inopposables les clauses de réciprocité et invalides les restrictions à la compétence de l'organe de contrôle qu'est la nouvelle Cour européenne des droits de l'homme.

L'ordre public européen impose au fond une véritable « exception » qui vise notamment à assurer la primauté de la Convention sur toute autre

forme de collaboration internationale à laquelle peut recourir l'Etat et à écarter les actes étrangers en contrariété avec la Convention.

Le professeur Sudre ne pouvait dès lors terminer son analyse de ce qui constitue l'essence même de la Convention européenne des droits de l'homme qu'en affirmant à raison que

« l'ordre public européen ne saurait s'accommoder de ce que ces valeurs puissent être méconnues sur le territoire d'un Etat partie, au motif que cette méconnaissance trouve sa source dans un jugement ou un acte étranger » (409).

Si l'on a en particulier égard à Echelon, tout est dit dans cette formule, sachant que

« caractéristique de l'Etat policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques » (410).

Le programme Echelon, au même titre que tous les cousins qu'il reste malheureusement à lui découvrir, dépasse largement cette mesure, ce qui le rend, pour peu que l'on puisse en juger en connaissance de cause, manifestement incompatible avec la *« prééminence du droit »* (411).

85. Echelon : une actualisation au 15 février 2001, mais un épilogue qui se fait toujours attendre (412) — La présente étude reposait sur une documentation à jour au 31 août 2000. L'affinement des recherches et la parution de plusieurs rapports nouveaux portant sur Echelon justifient une actualisation de cette documentation, étant entendu que divers contacts et conversations pris entre-temps n'ont fait que renforcer la conviction en la nécessité d'un argumentaire juridique le plus détaillé possible. Il est certain qu'Echelon a moins donné lieu, ces derniers mois, à l'efflorescence d'informations et supputations en tous genres (n° 6) (413). La meilleure synthèse ne pouvait émaner que de Duncan Campbell qui vient de publier en ce début 2001 un petit ouvrage reprenant l'essentiel de ces

(409) F. SUDRE, « Existe-t-il un ordre public européen », *op. cit.*, p. 79.

(410) Cour européenne des droits de l'homme, arrêt *Klass c. Allemagne* du 4 juillet 1978, § 42.

(411) Voyez P. WACHSMANN, « La prééminence du droit dans la jurisprudence de la Cour européenne des droits de l'homme », in *Etudes en l'honneur de J. Schwob*, Bruxelles, Bruylant, 1997, pp. 241-286.

(412) Les numéros de paragraphe indiqués en gras sont ceux de l'article actualisé ici. Il a été opté pour un texte d'actualisation suivi permettant la mise en contexte la plus récente des données disponibles sur Echelon et l'état du droit qui lui est applicable.

(413) Citons encore parmi les sites synthétisant régulièrement l'état de l'information sur Echelon : « <http://www.cyber-rights.org/interception/echelon> ». Parmi les nouvelles supputations, on rangera l'assertion de Mr G. BUTTARELLI, Secrétaire général de l'Autorité italienne de contrôle de protection des données, dans un projet de principes directeurs sur « La protection des données en relation avec la surveillance » en cours d'élaboration au sein du Conseil de l'Europe. Celui-ci note assez énigmatiquement, à propos du décalage entre prise de connaissance par le public et évolution technologique, que « lors de l'annonce du système 'Echelon 2', le système 'Echelon 1' n'avait pas encore été entièrement dévoilé » (« <http://www.coe.fr/dataprotection/frRapport%20buttarelli.htm> »).

travaux (414). Le journaliste a d'ailleurs été à nouveau auditionné par la commission temporaire du Parlement européen qui doit encore œuvrer durant le premier semestre 2001 (415). Les travaux de celle-ci seront sans doute plus que jamais déterminants pour l'avenir de la contestation d'Echelon alors que des plaintes diverses commencent à être formulées (416), d'une part, et que se poursuivent au moins trois enquêtes parlementaires en Belgique, en France et en Italie, d'autre part.

a) On doit relever **quelques nouveautés du côté des sources officielles des Etats participants à Echelon** ou, à tout le moins, des éléments s'ajoutant à ceux déjà recensés (n^{os} 7 à 9).

Si on prend le cas de l'**Australie**, force est de constater que le Parlement reçoit très peu d'éclaircissements sur les questions qu'il pose depuis une vingtaine d'années sur l'accord *UKUSA*, censé constituer l'ossature juridique d'Echelon (417). Une question écrite de 1980 n'eut droit qu'à une réponse laconique (418) ainsi qu'une autre en 1982 (419); un sénateur motiva longuement en 1987 une motion en faveur de la fermeture de la station de Pine Gap située en territoire aborigène et qualifiée de « *United States spy base* » mais le président de séance lui coupa la parole pour dépassement du temps imparti (420)... En juin 1999, Mr White, un responsable du *Defence Signals Directorate* (service de renseignement électronique australien) démentit, devant le comité parlementaire spécialisé, les allégations de la chaîne Channel 9 sur la collaboration illicite du service avec ses homologues américain et britannique et affirma que la vie privée des australiens était préservée. La chaîne avait pourtant interviewé Mr Brady, un autre responsable du service. La suite de la discussion mérite d'être reproduite tant elle indique l'ambiance dans laquelle les interrogations sont traitées :

« *Senator Hogg — Have any of our defence intelligence allies made representations to the government raising concerns over Mr Brady being the first person to admit the existence of the spying organisation called UKUSA?* »

Senator MacGibbon — That can hardly be true. Everyone knew it existed.

Mr White — Thank you, Senator MacGibbon. I was trying to find a way of making that point while sticking to the government's invariable policy. » (421).

(414) D. CAMPBELL, *Surveillance électronique planétaire*, Paris, Allia, 2001.

(415) Cons. ses interviews dans *Libération* 22.01.2001, *Le Soir* 25.01.2001 ou *Les Inrockuptibles* 06.02.2001.

(416) Une nouvelle plainte, contre X et contre l'Allemagne, les Etats Unis et le Royaume Uni, a été introduite par l'eurodéputée écologiste Ilka Schrauer au mois d'octobre 2000 : « <http://www.droit-technologie.org/2—print.asp?actu—id=-447227021&month=10&year=2000> ».

(417) Le site de recherche du Parlement australien est situé à l'adresse « <http://search.aph.gov.au> ». Tapez le terme de recherche « UKUSA ».

(418) Question du 02.12.1980 de Mr HOLDING, *House Hansard* 25.02.1981, p. 206.

(419) Question de Mr BULKUS, *Senate Hansard* 11.11.1982, p. 2208.

(420) Discussion en séance publique par Mr VALLENTINE, *Senate Hansard* 21.10.1987, p. 1047.

(421) Débats sur le budget de l'intelligence stratégique du Département australien de la défense, *Foreign Affairs, Defence and Trade Legislation Committee, Senate* 08.06.1999, p. 289.

La politique invariable du gouvernement correspondait jusqu'à ce très bref intermède à refuser de répondre aux questions sur l'accord UKUSA (422). Le sujet gêne manifestement les autorités australiennes puisqu'un débat qui se tint peu après tourna vite court lui aussi. Le professeur Ball, du *Strategic and Defence Studies Center* de l'Université de Canberra, était auditionné par le Comité sur les Traités du Sénat sur son rapport relatant le rôle des services de renseignement australiens lors de la crise de Timor. Le chercheur expliquait que la station électronique britannique de Hong Kong, surveillant les satellites chinois, ayant été fermée suite à la rétrocession à la Chine du territoire, ses agents furent réaffectés sur le site de la base australienne de Geraldton. Quand un sénateur lui demanda si un accord signé par le Département de la défense existait, le professeur Ball répondit qu'il s'agissait de l'accord UKUSA et, à la question de savoir si le Parlement avait eu à en connaître, il répondit que l'accord était très hautement classifié (précisément : « *It sits in a vault in Russell Hill* »), formellement signé en 1948 après des négociations étalées en 1947. Le sénateur voulait poursuivre mais fut à nouveau coupé par le président du comité (423).

Mr Brady, ancien directeur du DSD qui aurait donc reconnu le rôle de l'Australie en 1999, fut auditionné le 3 mai 2000 par le Comité du Sénat sur la défense. Retranché derrière le traditionnel refus de confirmer ou infirmer les allégations sur le rôle de son service dans l'accord UKUSA et Echelon, il déclara que

« *Without commenting directly on whether or not the particular network you refer to exists in the form speculated in the European Parliament report, we are satisfied that the intelligence arrangements that we have with the United States are strongly to Australia's benefit* » (424).

Les inquiétudes manifestées par un sénateur lors des débats sur l'adaptation de la législation australienne sur les télécommunications, craignant qu'Echelon ne constitue un cheval de Troie chez leurs alliés pour les services américains, ne regurent aucun écho (425).

Même si le degré d'information des Parlements des Etats participants à Echelon ravive les inquiétudes, il convient de rajouter au nombre des indices concordants, faisant suite au rapport 1996 du Vérificateur général du Canada, le rapport 1999-2000 du Commissaire du C.S.E. canadien (en français le Centre de sécurité des télécommunications) qui décrit une fois de plus ce qui ressemble à s'y méprendre à l'accord UKUSA :

(422) Adde la question de Mr CHIPP, *Senate Hansard* 30.05.1985, p. 2901.

(423) Audition du Professeur Desmond BALL, *Joint Committee on Treaties, Senate* 09.08.1999, p. 6.

(424) Audition de Mr BRADY sur l'intelligence stratégique, *Foreign Affairs, Defence and Trade Legislation Committee, Senate* 03.05.2000, p. 128.

(425) Intervention de Mr BROWN, *Senate Hansard* 07.06.2000, p. 14775.

« le CST reçoit des renseignements électromagnétiques recueillis par d'autres gouvernements. Il fournit également à ceux-ci des renseignements qu'il a lui-même recueillis. Ces accords de partenariat avec les Etats Unis, le Royaume Uni, l'Australie et la Nouvelle Zélande ont été établis au cours de la Deuxième Guerre Mondiale et maintenus pendant toute la durée de la guerre froide » (426).

b) Les moyens de défense des services de renseignement américains sont désormais publics — On se souviendra que le Congrès américain avait adopté en 1999 une section 309 dans l'*Intelligence Authorization Act for Fiscal Year 2000* en vue d'obliger les agences américaines à faire le point sur les règles juridiques suivies dans le domaine des interceptions de télécommunications (427) (n° 7). Les conclusion finales du Congrès ont été élaborées en février 2000 mais ne sont toujours pas accessibles au public. Toutefois, des auditions ultérieures des directeurs de la NSA et de la CIA en date du 12 avril 2000 sont désormais disponibles.

Le Lieutenant-général Hayden, qui dirige la NSA, a ainsi expliqué devant le House Permanent Select Committee on Intelligence que le 4^e amendement de la Constitution, le *Foreign Intelligence Surveillance Act* de 1978 et l'Ordre présidentiel n° 12333 de 1981 constitueraient autant de balises, l'interception des communications des citoyens américains étant défendue à la NSA, sauf autorisation du tribunal spécial instauré par le *FISA* et preuve de ce que l'écouté est un agent d'une puissance étrangère. Voilà pour le territoire américain, ce dispositif interdisant également qu'une agence étrangère ne collecte des renseignements que la NSA ne pourrait pas engranger à l'encontre de ses citoyens. L'interception en-dehors du territoire sur un ressortissant américain ne peut être ordonnée que par l'Attorney General (428).

La position exprimée par Mr Tenet, Directeur de la CIA, va dans le même sens :

« *Mr Chairman, I am here today to discuss allegations about SIGINT activities and the so-called Echelon program of the National Security Agency with a very specific objective : To assure this Committee, the Congress, and the American public that the United States Intelligence Community is unequivocally committed to conducting its activities in accordance with US law and due regard for the rights of Americans* ».

(426) Consultable sur le site officiel du CSE : « <http://csec-csst.gc.ca/reports/1999-2000/review-f.html> ». Le rapport affirme encore que chaque Etat a convenu de ne pas effectuer pour le compte d'un autre ce qui serait illégal dans ce dernier. On peut en déduire que si les 5 pays fondateurs ne s'écoutent pas l'un l'autre, ils ne peuvent donc orienter leurs appareils que sur le reste du monde...

(427) Ce sont bien les allégations sur Echelon qui avaient poussé le représentant américain Bob BARR à faire insérer cette section 309 (le texte de la proposition initiale et la justification émise devant la Chambre le 13 mai 1999 sont disponibles sur « <http://jya.com/echelon-barr.txt> »).

(428) Texte de la déposition du 12 avril 2000 du Lieutenant-général Hayden, consultable sur le site de la NSA : « <http://www.nsa.gov/releases/DIR-HPSCI-12Apr.pdf> ». Par « personne US », c'est-à-dire protégée, il faut entendre le citoyen US, le résident permanent étranger, les sociétés enregistrées aux USA.

Le Directeur Tenet nia tout espionnage industriel en affirmant premièrement, que les tâches de la CIA ressortent d'abord à la sécurité nationale, d'autres agences étant en charge du commerce; deuxièmement, qu'une telle activité irait à l'encontre du maintien de bonnes relations avec les alliés; et troisièmement, qu'il serait impossible de tracer des limites déterminant quelles sociétés devraient en bénéficier ou non. Si des informations économiques sont recueillies, c'est, selon le Directeur de la CIA, pour empêcher la violation des lois américaines ou que des sociétés américaines ne soient lésées, mais jamais pour procurer à celles-ci des avantages compétitifs injustes (429). Il n'en demeure pas moins que la collaboration des services de renseignement avec les entreprises américaines est sans cesse renforcée, que ce soit pour protéger les secondes des pratiques déloyales de leurs concurrentes étrangères, une des préoccupations majeures du rapport 1999 du Directeur de la CIA (430), ou en vue de développer les technologies permettant de traiter les informations disponibles sur Internet (431).

S'agit-il encore d'un démenti sur l'existence d'Echelon ou uniquement de sa dimension économique? Toujours est-il que toutes ces garanties ne concernent que les personnes américaines, de telle sorte que les voies de recours offertes par le droit américain à un citoyen étranger se plaignant d'interceptions de télécommunications sur un territoire étranger quel qu'il soit sont inexistantes et n'ont dès lors pas à être épuisées.

c) Le nouveau visage du droit britannique applicable aux services de renseignement — Le droit anglais se présente de manière sensiblement différente du droit américain. Il organise un recours devant une juridiction spécialisée, lequel est en principe ouvert à toute personne se plaignant d'un acte posé par les services de sécurité : il s'agit du tribunal créé par le *Regulation of Investigatory Powers Act 2000* (section 65 et annexe 3), lequel remplace les trois tribunaux spécialisés qui existaient jusqu'alors (432). Cette nouvelle loi très complexe est à lire en conjonction avec le *Human Rights Act 1998* dont la section 6 porte qu'il est illégal pour toute

(429) Texte de l'intervention le 12 avril 2000 du Directeur de la CIA devant le *House Permanent Select Committee on Intelligence*, sur le site de la CIA : « <http://www.cia.gov/cia/public-affairs/speeches/archives/2000/dci-speech-041200.html> ».

(430) G. TENET, *Annual Report for the United States Intelligence Community*, mars 2000, « <http://www.cia.gov/cia/publications/fy99intellrpt/dci-annual-report-99-16.html> » : « *Intelligence depends on adequacy of counterintelligence programs to provide warning and protective measures against both traditional espionage and non-traditional economic theft of US equities. Failure to protect our economic and security interests would impact America's prosperity at home and abroad* ».

(431) Discours de J.C. BANNON, Président du National Intelligence Council, prononcé le 6 octobre 2000 devant le Washington College of Law : « <http://www.cia.gov/cia/public-affairs/speeches/archives/-/gannon-speech-10062000.htm> ».

(432) Le *RIP Act 2000* remplace le tribunal créé par le *Interception of Communications Act 1985* (annexe 1), le tribunal instauré par le *Security Service Act 1989* (section 5 et annexe 1 qui s'appliquaient au seul service de renseignement intérieur ou MI5), celui mis en place par l'*Intelligence Services Act 1994* (annexe 1, qui était notamment applicable au MI6 — service de renseignement extérieur ou Special Intelligence Service — et au GCHQ — service de renseignement électronique —).

autorité publique britannique de poser un acte en contrariété avec la Convention européenne des droits de l'homme, d'une part, et la section 7 qui dispose qu'une personne qui est ou serait victime d'une telle violation — et ce, au sens de l'article 34 de la Convention — peut saisir les juridictions britanniques, en ce compris, s'il échet, une juridiction spécialisée comme celle créée par le RIPA.

Le système britannique peut paraître plus protecteur des droits fondamentaux. Mais le problème de la participation de services britanniques, spécialement le GCHQ (433), à des interceptions extra-frontalières de télécommunications, en particulier à partir de la base anglo-américaine de Menwith Hill, reste entier. Une personne résidant sur un territoire sous juridiction britannique est certes censée épuiser les voies de recours internes ainsi offertes. Il en va tout autrement des personnes qui ne sont pas sous la juridiction britannique de façon valable au regard du droit international (n^{os} 69-71), sachant de surcroît que, d'après le service de renseignement intérieur — le MI5 —, aucune des 275 plaintes introduites entre 1989 et 1997 devant le tribunal instauré par le *Security Service Act 1989* n'a été retenue (434). Ceci peut raisonnablement faire douter de l'effectivité des recours britanniques, à plus forte raison s'ils avaient à être actionnés par une personne résidant sur un territoire étranger, ce qui constitue une circonstance également de nature à dispenser de l'obligation d'épuiser ces recours (n^o 72). Car, outre le refus des autorités américaines et britanniques de confirmer ou infirmer l'existence d'Echelon, on sait désormais qu'elles refusent également de participer aux procédures d'enquête ou d'information actuellement menées par le Parlement européen et divers Parlements nationaux. Cet élément est déterminant aussi pour l'argument soutenant l'existence de pratiques administratives, troisième circonstance de nature à relever de l'obligation d'épuiser les voies de recours britanniques (n^o 75). La participation du GCHQ à Echelon, quelle que soit la portée réelle ou supposée de ce système, service dont la mission est intrinsèquement extra-territoriale (435), ne peut se concevoir qu'avec l'aval du Secrétaire d'Etat britannique, ce qui tend à indiquer la tolérance officielle (436).

(433) Le site central d'information du Gouvernement britannique affirme que « *GCHQ derives signal intelligence by monitoring a variety of communications and other signals, such as radars. For this purpose it controls and administers the Composite Signals Organisation which operates from a number of locations in the UK and overseas. Like SIS and the Security Service, it also works with a range of foreign intelligence and security services* » (« <http://www.cabinet-office.gov.uk/cabsec/1998/cim/cimrep3.htm> »).

(434) Information publiquement disponible sur le site du MI5 : « <http://www.mi5.gov.uk/acct4.htm> ».

(435) Outre la prévention et la détection de la grande criminalité ainsi que la préservation de la sécurité nationale, il est compétent, aux termes de la section 3, (2), (b), de l'*Intelligence Services Act 1994*, « *in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands* ».

(436) La section 7 de l'*Intelligence Services Act 1994* organisait une procédure détaillée d'autorisation par le Secrétaire d'Etat des actes à accomplir en-dehors du territoire. Il est évidemment

La nouvelle configuration du droit britannique, quand bien-même serait-il respecté par les services chargés de l'appliquer, ne saurait donc habilitier ceux-ci à procéder à des interceptions contraires à l'article 8 de la Convention européenne des droits de l'homme et à la souveraineté territoriale d'autres Etats. Surtout que les enquêtes parlementaires en cours dans d'autres pays vont dans le sens de la confirmation de l'existence d'Echelon.

d) Parmi les conclusions des **nouvelles enquêtes menées par les parlements nationaux**, on doit relever celles, relativement circonspectes, du **Comité parlementaire italien des services d'information**. Dans un rapport du 29 novembre 2000, celui-ci confirme qu'une base américaine d'interception située à San Vito dei Normanni a fonctionné jusqu'en 1993 avec l'aval des autorités italiennes sans avoir été dirigée en aucune manière contre des intérêts italiens. Le Comité italien se borne à affirmer que, si un accord de collaboration anglo-saxon en matière de renseignement électronique existe bien depuis la Deuxième Guerre Mondiale, aucune preuve n'atteste de son caractère mondial ni de ce qu'il s'occuperait d'autre chose que des communications par satellites, d'autre part. Ce rapport se contente également d'entériner l'affirmation américaine selon laquelle l'éventuelle captation d'informations à caractère économique respecterait la législation américaine, ce qui, faut-il le rappeler, quand bien même cela serait-il vrai, ne saurait conférer une quelconque validité aux écoutes menées au-delà de la juridiction territoriale américaine. Le peu d'entrain des autorités italiennes à enquêter plus avant découle vraisemblablement de ce que des responsables du SISMI (service d'information et de sécurité militaire) ont reconnu, sans plus de précisions, avoir bénéficié d'informations en provenance d'interceptions électroniques (437). A défaut d'être rassurant, cela a le mérite d'être clair.

e) **Par contre, l'existence d'Echelon ne semble plus faire aucun doute pour le Comité R belge** — Comme cela avait déjà été esquissé, le rapport complémentaire d'activités 1999 du Comité R que la commission parlementaire mixte Chambre — Sénat a fait sien courant 2000 comporte plusieurs enseignements (n° 11). Le premier est le manque de moyens des services belges pour protéger les communications sur le territoire ainsi que l'absence de politique gouvernementale en la matière. Mais, comme se le

inconcevable que chaque interception opérée par le GCHQ fasse l'objet d'une autorisation séparée. Soit le droit anglais n'est pas respecté à la lettre (serait-ce le cas, un acte de contrainte autorisé par le droit interne ne peut de toute façon violer la souveraineté territoriale d'un autre Etat) mais le GCHQ a l'aval du Gouvernement, soit cela se fait sans son aval mais il n'a alors pris aucune mesure pour éviter la perpétuation des violations du droit international et de la Convention européenne des droits de l'homme.

(437) Conclusions du rapport du Comité parlementaire des services d'information, de sécurité et de réglementation du secret d'état sur *Le rôle des services de renseignement et la sécurité dans le cas 'Echelon'*, 29 novembre 2000, doc. Chambre des Députés et Sénat de la République, XIII^e législature, XXXIV, n° 7. Ce document remis aux membres de la Commission temporaire du Parlement européen sur « Echelon » est référencé PE 294.998 et accessible via le site de celle-ci : <http://www.europarl.eu.int/meetdocs/committees/temp/20010122/temp20010122.htm> ».

demande le quotidien *Le Soir*, on peut aussi s'interroger sur le pourquoi de la présence d'un fonctionnaire de la Sûreté de l'Etat aux séminaires conjoints du FBI et de plusieurs services européens sur les interceptions de télécommunications, alors que la Sûreté n'a aucune prérogative légale en la matière (n° 35) (438). Par ailleurs, le commandant du Service Général de Renseignement de l'armée a bien affirmé que « suivre » Echelon en Belgique serait illégal faute d'habilitation des services belges leur permettant de procéder à des écoutes administratives (439).

Si on peut déplorer que les services belges soient démunis pour faire face aux menaces électroniques ainsi que le manque d'intérêt du comité ministériel du renseignement, on ne peut aussi que regretter la faiblesse de leur utilisation des sources ouvertes. L'effort d'information du Parlement belge a, en effet, été essentiellement accompli par MM. Y. Pouillet et J.-M. Dinant des Facultés Universitaires Notre-Dame de la Paix de Namur, mandatés comme experts par le Comité R. Leurs recherches récentes, qui portent également sur les violations de la vie privée des consommateurs par certaines entreprises actives sur Internet (440), tendent à relativiser la portée globale d'Echelon mais affirment avec force que les communications transitant par satellite peuvent parfaitement être interceptées, en particulier sur le site de Menwith Hill dont la localisation en fait le nœud essentiel du réseau anglo-saxon.

Il faut surtout souligner que l'analyse juridique de MM. Pouillet et Dinant va dans le même sens que celle développée dans la présente étude. Aux impératifs imposés par l'article 8 de la Convention européenne des droits de l'homme (les trois conditions de légalité, légitimité et nécessité dans une société démocratique que doivent remplir les interceptions de communications), les auteurs rajoutent à raison le respect de la souveraineté territoriale mais également le principe de précaution dont on sait qu'il constitue un autre sujet de discord transatlantique (441). Si la commission parlementaire fait siennes les conclusions de ces experts sur l'existence d'Echelon (442), le débat sur l'éventuelle saisine par le Gouvernement belge

(438) *Le Soir* 25.01.2001. Le Conseil des Ministres approuva bien le 24 novembre 1995 un avant-projet de loi visant à autoriser, dans certaines conditions et uniquement en cas d'échec d'autres modes d'enquête, le recours aux écoutes administratives par les services de renseignement (voy. le compte-rendu analytique de la Commission de la Justice de la Chambre du 6 décembre 1995, séance de l'après-midi). Mais le dossier en est resté là.

(439) Une traduction hâtive nous a fait écrire dans l'article paru au *J.T.D.E.* 2000, p. 190, note 45, qu'« Echelon serait illégal en Belgique ». L'affirmation reste juridiquement exacte mais n'a pas été formulée par le lieutenant-général MICHAUX.

(440) *Le Soir* 25.01.2001 ainsi que *La Lanterne* 25.11.2000 et *La Libre Belgique* 26.11.2000. (441) Voyez le rapport complémentaire d'activités 1999 du Comité permanent de contrôle des services de renseignements et de sécurité, fait par M. HORDIES et M^{me} PELZER-SALANDRA, 19 juillet 2000, *Doc. parl.*, Chambre 50 0813/001 et Sénat 2-513/1. Le rapport n'a toutefois été rendu public qu'à la fin octobre 2000.

(442) D'après nos informations, le Comité R serait en train de préparer un 3^e rapport sur Echelon qui n'est accessible qu'aux membres de la commission parlementaire mixte.

de la Cour européenne des droits de l'homme à l'encontre de l'Allemagne et du Royaume Uni demeure toujours pendant (n^{os} 12 et 13).

f) **Le rapport de la mission française d'information parlementaire confiée à Mr Paecht a été pour sa part rendu public en octobre 2000 (n^o 10)** — Le refus d'entrevue opposé au député français par les autorités américaines et britanniques n'a eu pour effet que de renforcer les présomptions sur l'existence d'Echelon. Le rapport « *Paecht* » n'apporte sur le fond que peu d'éléments nouveaux mais s'interroge utilement sur les conditions dans lesquelles ont été faites les révélations sur Echelon. On doit cependant déplorer de nouvelles approximations dans le traitement juridique du dossier. Si le rapport pose à raison la contrariété d'Echelon avec l'article 8 de la Convention européenne des droits de l'homme — sans mentonner toutefois la jurisprudence de l'année 2000 —, il n'en est pas moins parfaitement erroné d'écrire qu'

« Il n'y a pas de réglementation européenne des écoutes et des interceptions de communications privées. Les seuls textes existants n'ont pas de caractère contraignant et reflètent seulement une orientation politique. (...) Comme la Convention signée à Strasbourg le 28 janvier 1981, elle [la CEDH] ne contient pas de règles directement applicables dans l'ordre juridique interne des Etats membres mais énonce des principes que les Etats s'engagent à respecter en accordant leur législation à ces principes » (443).

S'il est un pays dans lequel l'article 8 de la Convention a un effet direct, c'est bien la France! La confusion ainsi opérée entre effet de la Convention au bénéfice des particuliers qui peuvent l'invoquer devant les juridictions internes et introduire une requête devant la Cour de Strasbourg, d'une part, et choix des moyens par les Etats pour se conformer à un éventuel arrêt de la Cour de Strasbourg constatant une violation, d'autre part, est regrettable en ce qu'elle montre une méconnaissance des ressources offertes par une Convention dont on ne dira jamais assez qu'elle doit être appréhendée en tant que système général de protection (n^o 18).

Il est toutefois un élément important qu'apporte le rapport « *Paecht* ». Celui-ci confirme la statut de la base de Bad Aibling en Allemagne alors que l'on ne disposait jusqu'ici à son égard de moins d'informations qu'à propos de celle de Menwith Hill. Suite à la visite du site en mai 2000 par une délégation parlementaire allemande guidée par un conseiller juridique américain, le rapporteur qui a rencontré des interlocuteurs allemands note que

« Les services de renseignement de l'Allemagne ont désormais accès aux moyens d'écoutes pour évaluer les informations recueillies et utiliser ces moyens en fonction de leurs objectifs et de leurs priorités. Mais, à la question qui a été posée sur le contrôle réellement effectué par les autorités allemandes, il a été répondu que

(443) Point II, B, 1, b) du rapport d'information sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, présenté par Mr PAECHT, 11 octobre 2000, Doc. A.N., n^o 2623.

celui-ci n'était pas mis en œuvre puisque les relations germano-américaines reposaient sur la confiance » (444).

Si les autorités allemandes semblent faire confiance aux services américains en ce qui concerne leurs relations bilatérales, ne peut-on raisonnablement penser que cette confiance — ce laisser-faire? — est aussi de mise quand la NSA écoute autrui à partir du territoire allemand? Territoire sur lequel l'Allemagne est débitrice d'une obligation de vigilance aux termes du droit international général (n° 55), obligation renforcée en ce qui concerne les stipulations de la Convention européenne des droits de l'homme (n°s 48-49 et 57-58)... Les autorités allemandes doivent aussi être entendues par le Parlement européen.

g) Les travaux de la commission temporaire du Parlement européen sont programmés jusqu'à la fin juin 2001 — La commission a déjà procédé à plusieurs auditions (445) dont celle du représentant de la présidence (française) du Conseil européen qui, après avoir rappelé les termes, pour le moins mesurés, de la résolution prise en mai 2000 par celui-ci à propos des interceptions de télécommunications, a affirmé que

« Sans préjuger des résultats des investigations que vous menez, on peut remarquer que l'existence des capacités d'interception de télécommunications mises en place par les Etats Unis, avec le concours du Royaume Uni, du Canada, de la Nouvelle Zélande et de l'Australie n'est plus guère aujourd'hui contestée ».

Mr Paecht, rapporteur de la mission d'information parlementaire française, s'est montré encore bien plus péremptoire (446). La commission temporaire collabore avec les Parlements belge, français et italien mais Mr Coelho, son président, se plaint amèrement du refus des Parlements britannique et danois de participer à ses réunions (447). Pendant que la Commission poursuit ses travaux, d'autres instances communautaires ont réfléchi aux problèmes des interceptions extra-frontalières.

h) Les instances communautaires rappellent constamment la portée de l'article 8 de la Convention en matière d'interceptions de télécommunications — C'est ainsi bel et bien la jurisprudence de la Cour européenne des droits de l'homme, relative à l'article 8 de la Convention, qui a permis au groupe de travail « Article 29 » (448) de conclure à la contrariété avec le droit à la vie privée des systèmes d'interception des télécommunications n'ayant pas de statut juridique suffisamment clair, étant principalement visées la résolution du Conseil européen du 17 janvier 1995, mais également les mesures de coopération technique avec des Etats tiers

(444) Point I, D, I, a) du rapport « Paecht ».

(445) Plusieurs journalistes ont été auditionnés les 22 et 23 janvier 2001, doc. PE 294.995.

(446) Auditions de Mr MASUREL et de Mr PAECHT le 28 novembre 2000, doc. PE 294.994.

(447) Compte-rendu de la réunion des 20 et 21 novembre 2000, doc. PE 294.991/REV.

(448) Ce groupe de travail, institué par l'article 29 de la Directive 95/46/CE, rassemble les commissions de protection de la vie privée des Etats membres de l'Union et remet des avis aux instances communautaires.

qui ne sont pas soumis aux mêmes impératifs que ceux découlant de la Convention. De surcroît, c'est en ayant égard à la résolution du Parlement européen de septembre 1998 qui s'inquiétait d'Echelon que le groupe « Article 29 » discute la légitimité des interceptions dépassant le strict cadre de la sécurité nationale et condamne, surtout, les écoutes téléphoniques à caractère général et exploratoire dès lors qu'il y a ingérence dans la vie privée à chaque interception, chacune devant alors répondre séparément aux exigences de l'article 8 de la Convention (449). Le même groupe de travail condamne donc logiquement aussi la pratique du « sniffing », c'est-à-dire le contrôle du trafic des courriers électroniques sur un réseau, dès lors qu'il s'inscrit dans le cadre d'une surveillance générale (450).

Après une longue période d'attentisme qui lui a été souvent reprochée (n° 14), la Commission européenne a, enfin, adopté le 26 janvier 2001 une communication intitulée « *Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité* ». Celle-ci note que sa résolution de 1995, dont l'extension avait profondément divisé deux commissions du Parlement (n° 16, note 120, et n° 32), n'a toujours pas été réexaminée par le Conseil. Mais la Commission européenne n'a pu que répéter une fois de plus que

« Dans l'Union européenne, il existe un principe général de confidentialité des communications (et des données relatives au trafic). Les interceptions sont illégales, sauf autorisation prévue par la loi dans des cas précis où ces mesures sont nécessaires et justifiées par des finalités en nombre limité. Ce principe découle de l'article 8 de la Convention européenne des droits de l'homme, qui est mentionné dans l'article 6 du traité sur l'Union européenne, et plus précisément des directives 95/46/CE et 97/66/CE ».

La Commission, visant explicitement le cas Echelon, aborde désormais frontalement la question de principe :

« Toute exploitation des possibilités d'interception faite de manière abusive et sans discernement, en particulier à l'échelle internationale, poserait des problèmes sous l'angle des droits de l'homme et saperait la confiance du citoyen dans la société de l'information. La Commission s'est alarmée de certains rapports dont elle a eu connaissance sur de prétendus abus des moyens d'interception » (451).

2) **Frontières, cybercriminalité et droits de l'homme dans le droit européen** — Les Etats de l'Union européenne savent pertinemment que l'application extra-territoriale des lois et règlements d'un Etat viole le droit international quand elle concerne les activités des personnes physiques et

(449) Point 6 de l'avis 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications, D.G. 15 de la Commission Européenne, 3 mai 1999, doc. WP 18.

(450) Document de travail sur le respect de la vie privée sur Internet, 21 novembre 2000, doc. WP 37, pp. 36-37 et 43. Echelon et le système Carnivore interpellaient en particulier le groupe « Article 29 ».

(451) Communication de la Commission du 26 janvier 2001, COM (2001) 890 final, p. 18 et 20. Les mêmes considérations sont émises à propos de « la conservation systématique des données sur une large fraction de la population » (p 21).

morales relevant de la juridiction d'autres Etats (n^{os} 27-29 e.a.). Une résolution du Conseil européen de 1996 émit un tel reproche à l'égard des Etats Unis (452).

L'un des débats mêlant intimement principe de territorialité et droit à la vie privée, qui opposait justement l'Union aux Etats Unis a été entre-temps résolu, la première autorisant désormais en principe les transferts de données vers les seconds alors que de sérieux doutes avaient été émis sur le degré de protection accordé à la vie privée sur le territoire américain (453).

D'un autre côté, les négociations en vue de l'élaboration d'une Convention sur la cybercriminalité menées sous l'égide du Conseil de l'Europe doivent aboutir à la mi-2001. Le nouveau projet rendu public en janvier 2001 prévoit d'abord en ce qui concerne les interceptions de données informatiques que les futures parties (dont les Etats Unis) incriminent les interceptions intentionnelles et sans base juridique (article 3). Les perquisitions et saisies informatiques devraient être autorisées sur leur territoire par le droit de chaque partie (article 19) ainsi que, toujours sur leur territoire, la collecte en temps réel des données relatives au trafic et associées à des communications précises (article 20); il en va de même de l'interception de données relatives au contenu (article 21). La principale clause de sauvegarde réside dans l'article 15 de ce projet de Convention sur la cybercriminalité :

« L'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus par la présente section doivent être sujettes aux conditions et sauvegardes prévues par le droit interne de chaque Partie concernée, eu égard à la protection adéquate des droits de l'homme — notamment telle qu'elle est définie dans les instruments internationaux concernant les droits de l'homme — et, le cas échéant, à la proportionnalité du pouvoir ou de la procédure avec la nature et les circonstances de l'infraction ».

Ceci revient un peu à se payer de mots : le principe de proportionnalité est d'ores et déjà une composante essentielle des systèmes européen et universel de protection des droits de l'homme (n^o 42); la primauté des traités protecteurs des droits de l'homme sur les autres conventions internationales ne peut de toute façon tolérer qu'il en soit autrement (n^{os} 58 et 64); les Etats Unis, non signataires de la Convention européenne des droits de l'homme mais bien du Pacte international relatif aux droits civils et politiques, n'ont toutefois pas adhéré au protocole permettant les communica-

(452) Le Conseil européen, confronté aux lois américaines « d'Amato » et « Helms-Burton » (sanctions des autorités américaines à l'égard des sociétés non américaines traitant avec l'Iran et Cuba) a adopté, le 22 novembre 1996, une action commune, sur la base des articles J.3 et K.3 T.U.E., relative aux mesures de protection contre les effets de l'application extra-territoriale d'une législation adoptée par un pays tiers, *J.O.C.E.* n^o L 309, 29.11.1996, p. 7.

(453) Décision de la Commission du 27 juillet 2000 conformément à la directive 95/46/CE relative à la pertinence de la protection assurée par les principes de la sphère de sécurité et par les questions souvent posées y afférentes publiées par le Ministère du commerce des Etats Unis.

tions individuelles devant le Comité des droits de l'homme de l'ONU (n° 82).

Qui plus est, le chapitre III du projet de convention, relatif à la coopération internationale, ne comporte pas une telle clause de protection des droits de l'homme, même si la primauté de la Convention européenne des droits de l'homme devrait, logiquement, empêcher ses signataires d'en contourner les exigences si la coopération en matière de cybercriminalité était amenée à dépasser son « territoire ». Toujours est-il, malgré les reproches plus précis (454) qui pourraient être adressés aux dispositions sur l'information spontanée (article 28), la simplification des procédures d'entraide en cas d'absence d'autres accords internationaux (article 27), l'entraide en matière de mesures provisoires (articles 29 et 30), que les Etats ne modulent l'exercice de leur souveraineté dans le domaine de la cybercriminalité qu'en marquant, au minimum, leur accord par voie conventionnelle. C'est d'autant plus vrai pour ce qui concerne l'entraide à propos des pouvoirs d'investigation puisque, au cas où une Partie souhaiterait accéder aux données stockées sur le territoire d'une autre Partie requise, celle-ci ne peut procéder à la perquisition, la saisie ou la divulgation de ces données informatiques (article 31) qu'en se conformant au moins aux instruments internationaux pertinents sur la coopération internationale en matière pénale (article 24) (455). Autrement dit, en-dehors des conditions portées par le projet de Convention du Conseil de l'Europe sur la cybercriminalité, dont le préambule se place sous les auspices de la Convention européenne des droits de l'homme et du Pacte international relatif aux droits civils et politiques, aucune donnée informatique ne peut traverser les frontières à des fins d'enquête. Quant aux interceptions téléphoniques, elles ne sont donc plus autorisées par le projet du Conseil de l'Europe alors qu'une proposition antérieure visait explicitement à les permettre (n° 30).

Par contre, comme l'indique son rapport explicatif, la nouvelle Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne est bien le premier traité international — connu du public, serait-on tenté de dire — à traiter spécifiquement des interceptions de télécommunications, dont les conversations télé-

(454) Pour un premier commentaire juridique : E.M. GNING, « Le projet de convention européenne sur la criminalité dans le cyberspace », *Lex Electronica*, vol. 6-2, 2001, « <http://www.lex-electronica.org/articles/v6-2/gning.htm> ».

(455) La 25^e version déclassifiée du projet de Convention sur la cybercriminalité date du 9 janvier 2001. Elle est disponible sur le site du Conseil de l'Europe : « <http://conventions.coe.int/treaty/FR/projets/cybercrime25.htm> ». L'accès transfrontalier à des données stockées sur un autre territoire que celui de la Partie requérante sans autorisation de l'autre Partie concernée n'est permis que si ces données sont accessibles au public ou si la personne légalement autorisée à divulguer des données confidentielles y consent volontairement (article 32). De même, une Partie requise ne peut assister une Partie requérante dans la collecte en temps réel des données relatives au trafic que si ces données étaient disponibles dans une affaire analogue au niveau interne (article 34), l'entraide quant à l'interception de données relatives au contenu ne se concevant que dans la mesure permise par les traités et le droit interne applicables (article 34).

phoniques ou les messages par telefax ou telex ou encore les courriers électroniques. Le projet du Conseil des Ministres avait été sévèrement amendé par le Parlement européen (n° 33). Les interceptions, dont le fruit sera transmis directement ou enregistré pour transmission ultérieure, peuvent être effectuées sur demande de l'autorité compétente d'un Etat membre par une autorité judiciaire ou administrative désignée par un l'Etat membre requis. On se situe certes ici dans le domaine de la coopération pénale, les écoutes administratives et par les services de renseignement n'étant manifestement pas concernées. Si aucune procédure spécifique de recours n'est prévue, c'est parce que les demandes doivent être traitées conformément au droit interne de l'Etat requis.

Mais la Convention relative à l'entraide judiciaire en matière pénale autorise cependant, malgré les critiques antérieures du Parlement européen, l'interception de télécommunications sur le territoire d'une autre partie, sans l'assistance technique de celle-ci, lorsqu'y est située une station satellite terrestre et pour peu que les fournisseurs d'accès dans l'Etat requérant en aient les capacités techniques. Il se peut également qu'une interception se poursuive sur le territoire d'un autre Etat en raison du déplacement de la cible : si son assistance technique n'est pas requise, il s'impose d'informer cet Etat que l'interception a eu lieu (456). On pourrait certes considérer que les Etats membres de l'Union qui ratifieront cette Convention auront préservé leur souveraineté territoriale en consentant ainsi à certains cas d'interceptions extra-frontalières. On objectera au contraire que la notification *a posteriori* déroge notablement aux mécanismes traditionnels de coopération judiciaire et policière. On peut par ailleurs douter une fois de plus de la manière de rencontrer les prescrits des articles 8 et 13 de la Convention européenne des droits de l'homme, notamment en ce qui concerne l'obligation de notifier aux personnes intéressées qu'elles ont fait l'objet de mesures d'interception et de leur ménager les recours idoines (457).

Le projet du Conseil de l'Europe, en son état au 9 janvier 2001, et la Convention UE du 29 mai 2000 (458), ne sont censément applicables qu'à

(456) Voyez sur les articles 17 à 21 de la Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, le rapport explicatif approuvé le 30 novembre 2000 par le Conseil européen, *J.O.C.E.* n° C 379 du 29.12.2000, pp. 20-26.

(457) En effet, devant quelles autorités contester : celles de l'Etat requérant ou de l'Etat requis ? Par ailleurs, tant qu'un Etat n'a pas réagi à la notification de ce qu'une interception a eu lieu sur son territoire, l'Etat interceptant ne peut utiliser les données interceptées, ce qui paraît déjà largement illusoire, à moins qu'ils n'en aient convenu autrement à deux ou encore pour prévenir un danger immédiat et sérieux pour la sécurité publique. Ce dernier cas de figure requiert un encadrement sévère par l'article 8 de la Convention européenne des droits de l'homme.

(458) Cette Convention relève des politiques dites du troisième pilier, plus particulièrement de la justice et des affaires intérieures, et se situe donc en-dehors des compétences des instances communautaires proprement dites. Ceci n'empêche pas la Commission européenne d'estimer que « les règles d'interception qui figurent dans cette convention d'entraide sont, pour l'heure, le maximum que l'on puisse envisager » (communication COM(2001) 890 final, précitée, p. 19).

certaines affaires particulières, sans caractère général ni exploratoire, d'une part, et dans le respect des textes internationaux protecteurs des droits de l'homme, d'autre part. Quelles que soient les critiques pouvant leur être adressées, ces deux textes n'en rappellent pas moins que la souveraineté territoriale demeure ce qu'elle est. La souveraineté continue dès lors à s'opposer aux actes de contrainte extra-territoriaux auxquels n'ont pas consentis les Etats sur le territoire desquels se trouvent les données ou sur lesquels transitent ou sont tenues des conversations téléphoniques et assimilées (459); *a fortiori* quand il s'agit des interceptions téléphoniques qui seraient l'apanage d'Echelon et des systèmes similaires. A moins d'être virtuellement inutiles, les deux textes montrent également que les interceptions extra-frontalières sont techniquement parfaitement réalisables (460). Mais, maintenant que les Etats signataires de la Convention européenne des droits de l'homme vont vraisemblablement appliquer dans les prochaines années les nouveaux traités internationaux sur la cybercriminalité et intensifier l'usage des nouvelles technologies en matière d'entraide judiciaire, ils devront garder à l'esprit sa primauté sur leurs autres engagements internationaux (461).

j) La pertinence de la jurisprudence de la Cour européenne des droits de l'homme ne s'est nullement démentie — L'arrêt *Messina contre Italie* du 28 septembre 2000 a une nouvelle fois rappelé, à propos du courrier des détenus, que les restrictions apportées à la liberté de correspondance devaient reposer sur un texte légal clair et accessible (462) (n^{os} 36 et suiv.). Le même arrêt a de plus établi une violation de l'article 13 de la Convention en raison du manque d'effectivité des voies de recours offertes en l'espèce.

(459) Le rapport explicatif (p. 24) est au demeurant très explicite sur ce qu'en-dehors des hypothèses prévues par la Convention, soit les enquêtes pénales, les principes généraux du droit international ne sont pas affectés par elle.

(460) Quant au droit belge, la loi sur la criminalité informatique a été sanctionnée et promulguée le 28 novembre 2000 (*Mon. b.* 03.02.2001). Le Parlement a persisté dans sa volonté de permettre les saisies de données informatiques situées sur un autre territoire dans des conditions que le Conseil d'Etat estimait à juste titre contraires au principe de souveraineté (article 8 de la loi, insérant un nouvel article 88ter dans le Code de procédure pénale) (n^o 31). Cependant, la Convention sur l'entraide judiciaire en matière pénale n'est pas encore entrée en vigueur et, si tant est qu'elle soit à l'abri des critiques, ne concernera au plus que l'ensemble des Etats membres de l'Union. Quant au projet de Convention sur la cybercriminalité du Conseil de l'Europe, il est toujours en cours de négociation. L'article 14 de la loi pose de surcroît un problème de compatibilité avec l'article 8 de la Convention européenne des droits de l'homme dans la mesure où le délai minimal de conservation des données sur le trafic est de 12 mois, lequel peut être allongé par simple arrêté royal (voyez les remarques en ce sens du Groupe de travail « Article 29 » à propos du respect de la vie privée sur Internet, doc. WP 37 précité). Le Sénat, à nouveau saisi aux termes d'une longue « navette » avec la Chambre, n'a pu réduire ce délai (rapport de Mr ISTASSE et M^{me} KACAR sur le projet de loi relative à la criminalité informatique, *Doc. Parl.*, Sénat, s.o. 2000-2001, n^o 2-392/9).

(461) L'arrêt *Cantoni c. France* du 15 novembre 1996, § 30 avait en effet posé que la circonstance qu'un texte interne s'inspire d'un texte communautaire ne peut faire « écran » au contrôle de la compatibilité avec la Convention des actes de l'Etat concerné.

(462) Arrêt *Messina c. Italie* du 28 septembre 2000, § 81.

La place de l'article 13 dans l'ordre juridique de la Convention est devenue à ce point importante qu'elle a justifié un revirement de jurisprudence autorisant désormais d'invoquer cette disposition en vue d'obtenir des voies de recours pour contester le caractère déraisonnable du délai d'aboutissement des procédures judiciaires (463). La Convention trouve progressivement dans le droit à un recours effectif un nouveau centre de gravité (n° 48). La meilleure illustration en est une condamnation récente de la Bulgarie en raison du refus de la Cour suprême de contrôler un pouvoir discrétionnaire illimité du pouvoir exécutif (464). La Cour de Strasbourg a surtout contribué ces derniers mois à consolider sa jurisprudence sur l'obligation pour les Etats parties de prévenir les violations de la Convention et, s'il échet, d'enquêter et sanctionner celles-ci. Le rappel a été opéré dans des affaires de traitements inhumains infligés par la police cypriste (465) ou par la section anti-terroriste turque (466). Ces principes ont clairement reçu application dans des affaires de destruction d'habitations par la gendarmerie en violation de l'article 8 de la Convention, l'article 13 étant également violé en raison de l'absence d'enquête effective (n° 49) (467).

Sur le plan procédural, on retiendra que la Cour, statuant sur la recevabilité d'une requête, a soulevé d'office la violation de l'article 8 dans une affaire de restriction de la correspondance d'un délinquant placé dans une institution psychiatrique en estimant que le délai de six mois, requis par l'article 35, § 1^{er} de la Convention, ne commençait à courir qu'une fois que la situation contestée prenait fin (468). La Cour a donc confirmé que l'hy-

(463) Arrêt *Kudla c. Pologne* du 26 octobre 2000 qui motive longuement ce revirement puisque, jusque là, la Cour considérait l'article 13 comme moins porteur de garanties pour le droit à un procès équitable que l'article 6.

(464) En l'occurrence, il s'agissait du refus d'enregistrer les statuts d'une association religieuse : arrêt *Hassan et Tchaouch c. Bulgarie* du 26 octobre 2000. Cette jurisprudence confirme la circonspection avec laquelle est accueillie la théorie de l'acte de gouvernement par la Cour.

(465) Arrêt *Egmez c. Chypre* du 21 décembre 2000 (violation de l'article 13, le parquet n'ayant pas réagi à la saisine du médiateur par l'intéressé).

(466) Arrêt *Büyükdag c. Turquie* du 21 décembre 2000 (violation de l'article 13 en raison de la non réouverture de l'enquête malgré l'apport d'éléments nouveaux). Le Comité des droits de l'homme va exactement dans le même sens d'un renforcement de l'obligation de mener une enquête effective : décision du 25 octobre 2000, com. n° 821/1998, *Chongwe c. Zambie*, point 5.3.

(467) Arrêt *Bilgin c. Turquie* du 16 novembre 2000, § 108 et 114 sv. Les multiples constats de violation dans cette affaire ont mené la Cour à se dispenser de vérifier si ces manquements s'inscrivaient dans un ensemble plus large de « pratique des autorités » (n° 74 quant aux pratiques administratives). Une affaire en tous points semblable a été jugée aussi dans l'arrêt *Dulas c. Turquie* du 30 janvier 2001 à propos duquel l'opinion dissidente du juge Gölcükdü, si elle admet que les voies de recours internes ne devaient pas être épuisées au sens de l'article 35, conteste le constat de violation de l'article 13 au motif que les plaignants ne se sont pas adressés une seule fois aux tribunaux. C'est cependant précisément dans ce dernier aspect que réside l'intérêt de la nouvelle jurisprudence de la Cour, lorsque sur les plans procédural (article 35) et substantiel (article 13), l'inefficacité des recours (éventuels) est telle qu'elle lève l'obligation de les épuiser et viole le droit de disposer des recours adéquats. Cette jurisprudence permet en effet de contester directement l'échelon devant la Cour de Strasbourg puisque les Etats participants continuent à nier son existence et sa portée.

(468) Décision de recevabilité de la Cour du 16 mars 2000, *Valle c. Finlande*, req. n° 28.808/95, affaire clôturée par arrêt du 7 décembre 2000 constatant le règlement amiable.

pothèse de la violation continue de la Convention relevait de l'obligation d'introduire les requêtes endéans les six mois de la décision interne définitive (n° 76). Quant à l'épuisement préalable des voies de recours internes en principe imposé par l'article 35, § 1^{er}, la jurisprudence la plus récente réaffirme qu'il ne peut s'interpréter avec un formalisme excessif (n° 67) (469). Pour les raisons exposées plus haut, l'adaptation récente des voies de recours contre les actes des services de renseignement en droit britannique ne saurait cependant les transformer en recours effectifs au sens de l'article 13 de la Convention, ni en recours à épuiser préalablement au sens de l'article 35, en particulier parce que le droit britannique ne peut s'appliquer en-dehors de ses frontières (*supra*, n° 85, c)).

Quant au Comité des droits de l'homme de l'ONU, il n'a toujours pas eu à se prononcer sur des affaires d'écoutes téléphoniques. Il a cependant établi qu'un Etat pourrait être tenu pour responsable des actes de particuliers qui auraient des conséquences en contrariété avec le Pacte international relatif aux droits civils et politiques (470). Ceci confirme que l'Etat peut engager sa responsabilité internationale de manière médiate en raison d'un acte ou une omission propre en rapport avec le comportement d'une personne tierce (nos 56-58). Le Comité a d'un autre côté singulièrement restreint la portée de sa jurisprudence *Casanovas* qui semblait permettre de porter devant lui une affaire qui avait été préalablement été déclarée irrecevable par la Cour européenne des droits de l'homme (n° 83) (471). La jurisprudence de cette dernière demeure bien le meilleur moyen d'analyser et contrer Echelon.

k) **Le centre du débat est en définitive moins l'existence d'Echelon que sa portée réelle** — Le rapport « Wright » estimait début 1998 que toutes les formes de communications continentales étaient interceptées (n° 2). Les enquêtes de Duncan Campbell ou de MM. Pouillet et Dinant, comme les conclusions des rapports parlementaires français et italien, ramènent sans doute à de plus justes proportions les aptitudes prêtées à Echelon. Le principal problème auquel les structures de surveillance électronique sont confrontées tient par ailleurs dans la croissance exponentielle des informations et communications transitant chaque seconde dans le monde. Si les « Dictionary » d'Echelon n'ont sans doute pas la capacité, faute de technologie actuelle de reconnaissance vocale, de trier les conversations téléphoniques, il n'en demeure pas moins que l'état de la technologie permet par contre de faire le tri sur base de mots-clés apparaissant dans les courriers électroniques (472). Et que les conversations téléphoniques peuvent quand même être écoutées individuellement dès lors qu'une cible ou un ensemble

(469) Arrêt *Dulas c. Turquie* du 30 janvier 2001, § 44.

(470) C.D.H., décision du 2 novembre 2000, com. n° 949/2000, *Kesharjee c. Canada*, point 4.2.

(471) C.D.H., décision du 25 octobre 2000, com. n° 808/1998, *Rogl c. Allemagne*.

(472) J. RICHARDSON, « Desperately seeking signals », *The Bulletin of Atomic Scientists*, avril-mai 2000, pp. 47-51, « <http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html> ».

de cibles sont choisis (473). Les explications que le FBI a du fournir au Congrès américain à la rentrée 2000 sur le système Carnivore qui permet l'interception des courriers électroniques montrent que la technologie permet d'y procéder (474). De surcroît, n'importe quel moteur de recherche du type *Yahoo!*, *Lycos* ou *Alta Vista* est d'ores et déjà apte à fournir avec une rapidité stupéfiante les pages des sites Internet contenant les termes demandés. Un responsable de la Central Police University de Taiwan vient aussi de porter à la connaissance du public comment fonctionne un système automatique de collecte d'informations sur les activités criminelles déployées sur Internet (475).

Même si les prémices d'un contrôle total de la vie privée sont encore loin d'être toutes rencontrées, le 1984 de George Orwell ne ressort plus complètement au seul domaine de l'imaginaire (n° 1). Avant même que l'existence d'Echelon ne soit évoquée en Europe, certains romans anglo-saxons avaient déjà dépeint la collaboration entre la NSA américaine et le GCHQ britannique, s'échangeant des informations électroniques sur base de listes de mots-clés (476). Dans un roman récent, Echelon lui-même est d'ailleurs l'instrument privilégié de la traque par la NSA et la CIA de terroristes iraniens

(473) Faire la part de ce qui est captable et ne l'est pas demeure d'autant plus difficile qu'il y a fréquemment un décalage entre développement d'une technologie à des fins militaires ou de sécurité et sa propagation publique. Qui plus est, si rapports et enquêtes divers s'accordent pour estimer que les communications par satellite sont les plus exposées et les communications par fibre terrestre, en principe, les plus sûres, grande est la zone d'incertitude en ce qui concerne tous les autres modes de communication. Outre le cryptage, c'est une reconfiguration générale de l'architecture des réseaux de communications qui serait censée le mieux éviter les dérives d'une surveillance générale comme celle prêtée à Echelon puisque, même si l'on passerait actuellement d'une proportion de 2/3 à une de 40 %, une part importante du trafic Internet mondial continue à passer par les États Unis (voyez le rapport du député Chr. PAUL au Premier Ministre français, intitulé *Du droit et des libertés sur l'Internet — La corégulation, contribution française pour une régulation mondiale*, Paris, La Documentation Française, mai 2000, p. 21).

(474) Divers articles ont été consacrés à Carnivore par le quotidien *USA Today* au mois d'août 2000 : « <http://www.usatoday.com/life/cyber/tech/> ». Voyez l'audition le 28 juillet 2000 de l'association Electronic Frontier Foundation devant le Congrès qui explique en quoi même les communications terrestres peuvent être interceptées et pourquoi Carnivore a les potentialités d'être utilisé comme système de surveillance de masse (« <http://www EFF.org/Privacy/Surveillance/Carnivore/20000728-eff-house-carnivore.html> ». Le site Internet officiel du FBI, qui comporte des pages dédiées à Carnivore (le patronyme est ici publiquement assumé), préfère arguer du caractère « *chirurgical* » des interceptions et de la légalité du système qui requiert à chaque fois un mandat judiciaire pour être actionné (« <http://www.fbi.gov/programs/carnivore> »). On sera frappé par cette terminologie guerrière, un responsable du FBI auditionné le 6 septembre 2000 par le Congrès ayant justifié l'existence de Carnivore au nom notamment de l'« *Information Warfare* » (« <http://www.fbi.gov/pressrm/congress/congress00/herr090600.htm> »). Malgré la désignation d'un comité d'experts, les craintes des associations persistent (*Libération* 07-08.10.2000).

(475) P.S. CHEN, « An Automatic System for Collecting Crime Information on the Internet », *Journal of Information, Law and Technology*, n° 2000-3, « <http://elj.warwick.ac.uk/jilt/00-3/chen.html> ».

(476) Par exemple J. FINDER, *L'instant Zéro*, Paris, Robert Laffont, 1998, pp. 67-69, initialement publié à New York en 1996 sous le titre *The Zero Hour*. Ou encore M. SMITH, *L'espion qui dansait sur l'eau*, Paris, Le Livre de Poche, 2000, p. 349, publié la première fois en 1994 sous le titre *Stone Dancer*.

qui financent l'acquisition d'armes nucléaires par un trafic d'héroïne (477). Dans le monde de la fiction, l'ennemi est forcément antipathique et prêt à tout : la préservation des intérêts vitaux d'un Etat justifie facilement toutes les méthodes d'investigation. Dans le monde réel, une police pouvant perquisitionner n'importe où et n'importe comment, sera assurément plus efficace. En sera-t-elle plus démocratique ? Quant à l'espionnage économique, il est autant le fait des entreprises privées entre elles (478) que celui des Etats (479). De quoi réduire à néant la sacro-sainte liberté de concurrence reposant sur le mythe de la non-intervention de l'Etat en matière économique, surtout quand intérêts vitaux nationaux se confondent avec ceux des industries de la défense et des télécommunications, à moins que cela ne soit l'inverse. Mais la préoccupation majeure exprimée ici concerne avant tout les libertés individuelles.

S'il convient de ne nourrir aucune illusion à l'égard d'un programme secret qui n'est certainement pas unique en son genre, on ne saurait se contenter d'incantations sur le respect dû à la vie privée. Divers Parlements nationaux ainsi que le Parlement européen ont d'ores et déjà pris conscience de la contrariété d'Echelon avec ce droit fondamental. Par conséquent, l'établissement de la responsabilité internationale des Etats qui collaborent activement ou passivement à un tel réseau requiert, au minimum, la cessation des faits internationalement illicites et d'offrir des garanties de non-répétition appropriées (480). Dans tous les cas, qu'il s'agisse des Etats Unis ou des parties à la Convention européenne des droits de l'homme, l'obligation internationale violée est le respect dû la souveraineté territoriale des pays tiers. Et, en ce qui concerne les parties à la Convention, les obligations violées sont, de surcroît, ses articles 8 et 13.

Si la réalité rejoint la fiction, rappelons-nous que, pour les individus, un pan essentiel de cette réalité réside aussi dans la cohérence et l'effectivité sans précédent du système de la Convention européenne des droits de l'homme pris dans son ensemble, un système que tous les Etats parties doivent non seulement respecter mais aussi faire respecter.

(477) L. COLLINS, *Demain est à nous*, Paris, Robert Laffont, 1998, pp. 98 et 321-322, paru la même année en anglais.

(478) Sur l'inadéquation du droit français, que l'on peut transposer au droit belge, dans ce domaine, on lira avec fruit la thèse de J. DUPRÉ, *Pour un droit de la sécurité économique de l'entreprise. De l'espionnage industriel à l'intelligence économique*, présentée le 3 novembre 2000 à la Faculté de Droit et de Sciences économiques de l'Université de Nice — Sophia Antipolis.

(479) Outre les informations publiées dans le dernier ouvrage de Duncan CAMPBELL et l'enquête de la chaîne NBC du 14 avril 2000, voyez également à propos de la réorientation générale de l'Administration Clinton en direction du renseignement économique : S. KOBER, « Why Spy ? The Uses and Misuses of Intelligence », *Cato Policy Analysis*, n° 265, 1996, « <http://www.cato.org/pubs/pas/pa-265es.html> ».

(480) Nouvel article 30 du projet de la Commission du Droit International sur la responsabilité internationale des Etats provisoirement adopté en seconde lecture par le comité de rédaction, doc. off. A.G., 55^e session, supp. n° 10 (A /55/10), p. 109 (sur la manière dont les travaux de la CDI sont ici recensés : n° 53, note 293).