2-754/2 (Senaat)
DOC 50 **1660/002 (Kamer)**

Belgische Senaat en Kamer van volksvertegenwoordigers

ZITTING 2001-2002

25 FEBRUARI 2002

Verslag over het eventuele bestaan van een netwerk voor het onderscheppen van communicaties, «Echelon» genaamd

BIJLAGEN

Zie:
Stukken van de Senaat:
2-754 - 2001/2002:
Nr. 1: Verslag.
Stukken van de Kamer van volksvertegenwoordigers:
50-1660 - 2001/2002:
Nr. 1: Verslag.

2-754/2 (Sénat)
DOC 50 **1660/002 (Chambre)**

Sénat et Chambre des représentants de Belgique

SESSION DE 2001-2002

25 FÉVRIER 2002

Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé «Echelon»

ANNEXES

Voir:
Documents du Sénat:
2-754 - 2001/2002:
Nº 1: Rapport.
Documents de la Chambre des représentants:
50-1660 - 2001/2002:
Nº 1: Rapport.

BIJLAGE 1 (*) | **ANNEXE 1 (*)**

December 23. 1971

Number 5-6100.20

DEPARTMENT OF DEFENSE DIRECTIVE

— *SUBJECT:* The National Security Agency and the Central Security Service (U)

Reference: (a) National Security Council Intelligence Directive No. 6

I. PURPOSE

This directive prescribes authorities, functions, and responsibilities of the National Security Agency (NSA) and the Central Security Service (CSS).

II. CONCEPT

A. Subject to the provisions of NSCID No. 6, and the National Security Act of 1947, as amended, and pursuant to the authorities vested in the Secretary of Defense, the National Security Agency is a separated organized agency within the Department of Defense and under the direction, supervision, funding, maintenance and operation of the Secretary of Defense.

B. The National Security Agency is a unified organization structured to provide for the Signals Intelligence (SIGINT) mission of the United States and to insure secure communications systems for alle departments and agencies of the US Government.

C. The Central Security Service will conduct collection and processing and other SIGINT operations as assigned.

III. DEFINITIONS

A. *Signals Intelligence (SIGINT)* is a category of intelligence information comprising all Communications Intelligence (COMINT), Electronics Intelligence (ELINT), and Telemetry Intelligence (TELINT).

B. *COMINT* is technical and intelligence information derived from foreign communications by other than the intended recipients. COMINT is produced by the collection and processing of foreign communications passed by electromagnetic means, with specific exceptions stated below, and by the processing of foreign encrypted communications, however transmitted. *Collection* comprises search, intercept, and direction finding. *Processing* comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of results. COMINT shall not include:

1. Intercept and processing of unencrypted written communications, except the processing of written plain text versions of communicatios which have been encrypted or are intended for subsequent encryption.

2. Intercept and processing of press, propaganda and other public broadcasts, except for processing encrypted or «hidden meaning» passages in such broadcasts.

3. Oral and wire interceptions conductes under DoD Directive 5200.24.

4. Censorship.

C. *ELINT* is technical and intelligence information derived from foreign, non-communications, electromagnetic radiations emanating from other than atomic detonation or radioactive sources. ELINT is produced by the collection (observation and recording), and the processing for subsequent intelligence purposes of that information.

D. *TELINT* is technical and intelligence information derived from the intercept, processing, and analysis of foreign telemetry.

E. *SIGINT operational control* is the authoritative direction of SIGINT activities, including tasking and allocation of effort, and the authoritative prescription of those uniform techniques and standards by which SIGINT information is collected, processed and reported.

F. *SIGINT resources* comprise units/activities and organizational elements engaged in the conduct of SIGINT (COMINT, ELINT or TELINT) activities.

(*) *Bron:* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/04-01.htm | (1) *Source:* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/04-01.htm

VI. APPLICABILITY

The provisions of this directive apply to the Office of the Secretary of Defense, the military department, the Joint Chiefs of Staff, the unified and specified commands, the National Security Agency, the Central Security Service, and other Defense agencies hereinafter called Department of Defense components.

V. ORGANIZATION AND RESOURCES

A. The SIGINT resources of the Department of Defense will be structured to accomplish most efficiently and effectively the SIGINT mission of the US.

B. The National Security Agency shall consist of a Director, a Headquarters, and such subordinate units, elements, facilities, and activities as are assigned to the National Security Agency by the Secretary of Defense *in his role as the executive agent of the Government for he conduct of SIGINT.*

C. The Central Security Service is comprised of a Chief, Central Security Service, a Deputy Chief, a jointly staffed headquarters, Army, Navy/Marine Corps and Air Force Operating elements, and such other subordinate elements and facilities as may be assigned to the Central Security Service by the Secretary of Defense.

D. The Director, National Security Agency, shall also be the Chief, Central Security Service.

E. The Director of the National Security Agency/Chief, Central Security shall have a Deputy Director for the National Security Agency and a Deputy Chief, Central Security Service. To provide continuity in SIGINT matters the Deputy Director, National Security Agency, shall be a technically experienced civilian. The Deputy Chief, Central Security Service, shall be a commissioned officer of the military Services, of not less than two star rank, designated by the Secretary of Defense. The Deputy Chief will normally not be selected from the same military Service as the Chief.

F. *The Director and Deputy Director of the National Security Agency shall be designated by the Secretary of Defense, subject to the approval of the President.* The Director shall be a commissioned officer of the military Services, on active or reactivated status, and shall enjoy not less than three rank during the period of his incumbency.

G. *The Director, National Security Agency/Chief, Central Security Service shall report to the Secretary fo Defense.*

H. The Commanders of the Service cryptologic organizations andtheir subordinate activities which conduct SIGINT operations will be subordinate to the Chief, Central Security Service, for all matters involving SIGINT activities. In this role they will be designated as Service element commanders and subordinate activities of the Central Security Service. Unless otherwise specifically provided in this directive, the Service cryptologic organizations will remain in their parent Services, for the purpose of administrative and logistic support.

I. The Secretary of Defense with the advice of the Joint Chiefs of Staff may specifically designate other SIGINT-related resources of the Department of Defense which will be subordinate to the Chief, Central Security Service for SIGINT operations.

VI. RESPONSIBILITIES AND FUNCTIONS

A. Subject to the direction, authority and control of the Secretary of Defense, the Director, National Security Agency/Chief, Central Security Service shall:

1. Accomplish the SIGINT mission of the National Security Agency/Central Security Service.

2. *Act as principal SIGINT advisor to the Secretary of Defense, the Director of Central Intelligence, and the Joint Chiefs of Staff.* As principal SIGINT advisor to the joint Chiefs of Staff, the Director, National Security Agency will keep the Joint Chiefs of Staff fully informed on SIGINT matters.

3. Exercise SIGINT operational control over SIGINT activities of the US Government to respond most effectively to military and other SIGINT requirements. In the case of mobile military SIGINT platforms, she shall state movement requirements through appropriate channels to the military commanders, who shall retain responsibility for operational command of the vehicles.

4. Provide technical guidance to all SIGINT or SIGINT-related operations of the US Goverment.

5. Formulate programs, plans, policies, procedures and principles.

6. Produce and disseminate SIGINT in accordance with the objective, requirements and priorities established by the Director of Central Intelligence. *(This function will not include the production and dissemination of finished intelligence which are the responsibilities of departements and agencies other than the National Security Agency/Central Security Service.)*

7. Manage assigned SIGINT resources, personnel and programs.

8. *In relation to the Department of Defense SIGINT activites, prepare and submit to the Secretary of Defense a consolidated program and budget, and requirements for military and civilian manpower, logistic and communications support, and research, development, test and evaluation, together with his recommendations pertaining thereto.*

9. Conduct research, development and systems design to meet the needs of the National Security Agency/Central Security Service and coordinate with the departments and agencies their related research, development, test and evaluation in the SIGINT field.

10. *Determine and submit to the Secretary of Defense logistic support requirements for the National Security Agency, and the Central Security Service, together with specific recommendations as to what each of the responsible departments and agencies of the Government should supply.*

11. Develop requisite security rules, regulations and standards governing operating practices in accordance with the policies of the US Intelligence Board and the US Communications Security Board.

12. Prescribe within his field of authorized operations requisite security regulations covering operating practices, including the transmission, handling, and distribution of SIGINT material within and among the elements under his control; and exercise the necessary monitoring and supervisory control to ensure compliance with the regulations.

13. Make reports and furnish information ot the US Communications Intelligence Board on the US Communications Security Board, as required.

14. *Respond to the SIGINT requirements of all DoD* components and other departments and agencies.

15. Eliminate unwarranted duplication of SIGINT efforts.

16. Standardize SIGINT equipment and facilities wherever practicable.

17. Provide for production and procurement of SIGINT equipments.

18. *Provide the Director of Central Intelligence through the Secretary of Defense with such information as required on the past, current and proposed plans, programs, and costs of the SIGINT activites under his control.*

19. Provide guidance to the military departments to effect and insure sound and adequate military and civilian SIGINT career development and training programs, and conduct, or otherwise provide for, necessary specialized and avanced SIGINT training.

20. Provide technical advice and support to enhance SIGINT arrangements with foreign governments, and conduct, as authorized, SIGINT exchanges with foreign governments.

21. *Perform such other functions as the Secretary of Defense assigns.*

VII. AUTHORITIES

A. *Subject to the authority, direction and control of the Secretary of Defense, the Director, National Security Agency/Chief, Central Security Service, is specifically delegated authority to:*

1. *Exercise SIGINT operational control over SIGINT activities of the United States.*

2. Issue direct to any of his operating elements such instructions and orders necessary to carry out his responsibilities and functions.

3. Have direct access to, and direct communications with, any element of the US Government performing SIGINT functions.

4. The authority in paragraphs 1, 2 and 3 above is subject to review, approval and control in accordance with procedures determined by the Secretary of Defense.

5. Adjust as required, through the Service cryptologic organizations, personnel resources under his SIGINT operational control.

6. Centralize or consolidate SIGINT operations for which he is responsible to the extent desirable, consistent with efficiency, economy, effectiveness, and support to field commanders.

7. Submit, as appropriate, concurrent/letter of evaluation efficiency/fitness reports on the commanders of subordinate elements of the Central Security Service in accordance with parent Service procedures.

8. Delegate SIGINT operational tasking of specified SIGINT resources and facilities for such periods and for such operational tasks as required or as directed by the Secretary of Defense.

9. Prescribe SIGINT procedures for activities to whom he provides technical guidance.

10. Prescribe, or review and approve security rules, regulations and instructions, as appropriate.

11. Conduct those SIGINT operations undertaken in support of certain missions within the purview of NSCID No. 5.

12. Obtain such information and intelligence material from the departments and agencies (military departments, other Department of Defense agencies, or other departments of agencies of the Government) as may be necessary for the performance of the National Security Agency/Central Security Service functions.

13. Maintain a departmental property account for the National Security Agency and the Central Security Service headquaters.

B. Other authorities, specifically delegated by the Secretary of Defense or by other proper authority to the Director, National Security Agency/Chief, Central Security Service in other directives or issuances, will be referenced in an Inclosure to this directive.

VIII. RELATIONSHIPS

A. In the performance of its responsibilities and functions, the National Security Agency/Central Security Service shall:

1. Coordinate actions, as appropriate, with other DoD components, and other departments and agencies of the Government.

2. Maintain direct liaison, as appropriate, for the exchange of information and advice in the field of its assigned responsibility with other DoD components and other departments and agencies of the Government.

3. Coordinate with DoD components and other departments and agencies of the Government to make maximum use of established facilities to preclude unnecessarily duplicating such facilities.

4. Provide for direct liaison by representatives of the intelligence components of individual departments and agencies regarding interpretation and amplification of requirements and priorities within the framework of objectives, requirements, and priorities established by the Director of Central Intelligence.

B. Other DoD componentes shall provide support, within their respective fields of responsibility, to the Director, National Security Agency/Chief, Central Security Service as may be necessary to carry out his assigned responsibilities and functions.

IX. ADMINISTRATION

A. To the extent applicable and consistent with the functions assigned to the National Security Agency/Central Security Service, Department of Defense policies, regulations and procedures will govern.

B. The National Security Agency/Central Security Service will be authorized such personnel, facilities, funds and other administrative support as the Secretary of Defense deems necessary for the performance of its functions. Other DoD components shall provide support for the Agency/Service as prescribed in specific directives or support agreements.

X. CANCELLATION

To the extent they are inconsistent herewith, DoD Directive S-5100.20, «The National Security Agency», dated March 19, 1959, Dod Directive S-3115.4, «Communications Intelligence», dated March 19, 1959, and DoD Directive S-3115.2, «Electronics Intelligence», dated February 7, 1967 are hereby cancelled.

XI. EFFECTIVE DATE AND IMPLEMENTATION

A. This directive is effective upon publication.

B. To meet the provisions of this directive, the Director, National Security Agency will develop a plan to implement this directive including establishment of the Central Security Service for approval by the Secretary of Defense with the advice of the Joint Chiefs of Staff.

C. When the Central Security Service is established under the terms of this directive and the approved implementing plan, all Departement of Defense components will review their existing directives, instructions, and regulations for conformity and submit necessary amendments thereto to the Assistant Secretary of Defense (Intelligence) within ninety (90) days.

Secretary of Defense

LISTING OF SPECIFIC DELEGATIONS OF AUTHORITY BY THE SECRETARY OF DEFENSE TO THE DIRECTOR OF THE NATIONAL SECURITY AGENCY

1. Administrative authorities required for the administration and operation of the National Security Agency, as prescribed in DoD Directive 5100.23, dated May 17, 1967.

2. Authority to authorize or request the procurement of cryptologic material and equipment by the military departments, as prescribed in DoD Directive 5160.13, dated March 20, 1956.

3. Authority to establish and administer programs of training, as prescribed in DoD Directive 1430.4, dated August 5, 1969.

4. Authority to assign the classification of TOP SECRET, as prescribed in DoD Directive 5200.1, DoD info Security Prop. authorized by DoD Dir. 52001, June 2, 1977.

5. Authority to determine the eligibility of individual civilian officers and employees to transport or store their privately owned motor vehicles at Government expenses, in accordance with provisions of DoD Directive 1418.3, dated June 28, 1965.

BIJLAGE 2(*) | **ANNEXE 2(*)**

NAVAL SECURITY GROUP

(For Official Use Only upon removal of Enclosure).

NAVSECGRU INSTRUCTION C5450.48A.

From: Commander, Naval. Security Group Command

Subj: MISSION, FUNCTIONS AND TASKS OF NAVAL SECURITY GROUP ACTIVITY (NAVSECGRUACT) SUGAR GROVE, WEST VIRGINIA

Ref: (a) OPNAVNOTE 5450 Ser 09B22/2U510135 of 29 Jun 1992.

Encl: (I) Mission, Functions and Tasks of NAVSECGRUACT Sugar Grove, WV.

1. Purpose. To publish the functions and tasks of NAVSECGRUACT Sugar Grove under the mission established by reference (a).

2. Cancellation. NAVSECGRU Instruction C5450.48.

3. Mission. To perform Naval Security Group related functions as directed and to perform such other functions anD tasks as may be directed by higher authority.

4. Status and Command Relationships. NAVSECGRUACT Sugar Grove is a shore activity in an active (fully operational) status under a Commanding Officer and under COMNAVSECGRU.

a. Command: COMNAVSECGRU

Echelon

(1) Chief of Naval Operations

(2) Commander, Naval Security Group Command

(3) Commanding Officer, Naval Security Group Activity Sugar Grove West Virginia

b. Area coordination

Chief of Naval Education and Training (CNET) exercises

Area and Regional Coordinator responsabilities

c. Subordinate Commands

d. Tenant Commands

(1) NNMC Bethesda Branch Medical Clinic, Sugar Grove

(2) PSD Bethesda Customer Service Desk, Sugar Grove

(3) Detachment 3, 544th Intelligence Group

(4) Navy Exchange, Sugar Grove

5. Action. To accomplish the assigned mission, the Commanding Officer NAVSECGRUACT Sugar Grove will ensure performance of the mission, functions and tasks in enclosure (1). Send recommended changes via the chain of command to COMNAVSECGRU (N8).

Mission, Functions and Tasks of NAVSECGRUACT Sugar Grove

1. (U) Mission. To perform Naval Security Goup related functions as directed and to perform such other functions ans tasks as may be directed by higher authority.

2. (U) Functions and Tasks. The Commanding Officer, in carrying out the assigned mission of NAVSECGRUACT Sugar Grove, will:

a. (U) Perform the functions and accomplish the tasks

required by:

(1) The Director, National Security Agency/Chief,

Central Security Service in the exercise of

(2) (U) COMNAVSECGRU in the exercise of command of NAVSECGRUACT Sugar Grove

(3) (U) DIRNAVSECGRULANT, Norfolk, in the exercise of administrative control for cryptologic activities and resources. The Commanding Officer will report, in person or by letter, to DIRNAVSEC-GRULANT, Norfolk for additional duty involving these functions.

(*) *Bron:* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/09-01.htm | (1) *Source:* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/09-01.htm

(4) (U) CNET for matters deriving from the exercise of Area and Regional coordination responsibilities. For this purpose, the Commanding Officer wil report in person, or by letter, to the designated Area Coordinator for additional duty.

(5) (U) Interservice, intraservice or other agreements.

b. (U) Perform the following specific functions and tasks:

(1) (U) Maintain and operate an ECHELON site.

(2) Process and report intelligence information.

(3) (U) Ensure the privacy of US citizens are properly safeguarded pursuant to the provisions of USSID 18.

(4) Provide support to Director, as directed by COMNAVSECGRU.

(5) (U) Operate special security communications facilities, as directed.

(6) (U) Perform service tests on new equipment and conduct other technical measurements and studies.

(7) (U) Function as Special Security Officer (SSO) for NAVSECGRUACT Sugar Grove.

(8) (U) Provide administrative support for NAVSECGRU personnel assigned to non-NAVSECGRU shore commands in the area.

(9)

(10) (U) Liaise with NNMC Bethesda to ensure NNMC Bethesda Branch Medical Clinic, Sugar Grove is properly manned and equipped to meet mission requirements in support of NAVSECGRUACT Sugar Grove

(11) (U) Liaise with PSD Bethesda to ensure PSD Bethesda Customer Support Desk, Sugar Grove is properly manned and equipped to meet mission requirements in support of NAVSECGRUACT Sugar Grove

(12) (U) Liaise with the 544th Intelligence Group (IG) to ensure Detachment 3, 544th IG is properly manned and fully integrated into the Operations Department of NAVSECGRUACT Sugar Grove. Maintain command authority over Detachment 3, 544 IG.

(13) (U) Liaise with MEXCOM Norfolk, to ensure Navy Exchange, Sugar Grove is properly manned and supplied to meet customer service requirements in support of NAVSECGRUACT Sugar Grove.

(14) (U) Perform such other functions and tasks which are normal and inherent responsibilities of command, including tasks resulting from intraservice/interservice support agreements and memoranda of agreement/understanding.

Date of Source: 3 September 1991.

Created on 8 August 1996.

BIJLAGE 3 | **ANNEXE 3**

The Wall Street Journal, March 17, 2000

Why We Spy on Our Allies

By R. James Woolsey, a Washington lawyer and a former Director of Central Intelligence.

What is the recent flap regarding Echelon and US spying on European industries all about? We'll begin with some candor from the American side.

Yes, my continental European friends, we have spied on you. And it's true that we use computers to sort through data by using keywords. Have you stopped to ask yourselves what we're looking for?

The European Parliament's recent report on Echelon, written by British journalist Duncan Campbell, has sparked angry accusations from continental Europe that US intelligence is stealing advanced technology from European companies so that we can — get this — give it to American companies and help them compete. My European friends, get real. True, in a handful of areas European technology surpasses American, but, to say this as gently as I can, the number of such areas is very, very, very small. Most European technology just isn't worth our stealing.

Why, then, have we spied on you? The answer is quite apparent from the Campbell report — in the discussion of the only two cases in which European companies have allegedly been targets of American secret intelligence collection. Of Thomson-CSF, the report says: «The company was alleged to have bribed members of the Brazilian government selection panel.» Of Airbus, it says that we found that «Airbus agents were offering bribes to a Saudi official.» These facts are inevitably left out of European press reports.

That's right, my continental friends, we have spied on you because you bribe. Your companies' products are often more costly, less technically advanced or both, than your American competitors'. As a result you bribe a lot. So complicit are your governments that in several European countries bribes still are tax-deductible.

When we have caught you at it, you might be interested, we haven't said a word to the US companies in the competition. Instead we go to the government you're bribing and tell its officials that we don't take kindly to such corruption. They often respond by giving the most meritorious bid (sometimes American, sometimes not) all or part of the contract. This upsets you, and sometimes creates recriminations between your bribers and the other country's bribees, and this occasionally becomes a public scandal. We love it.

Why do you bribe? It's not because your companies are inherently more corrupt. Nor is it because you are inherently less talented at technology. It is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith. In spite of a few recent reforms, your governments largely still dominate your economies, so you have much greater difficulty than we in innovating, encouraging labor mobility, reducing costs, attracting capital to fast-moving young businesses and adapting quickly to changing economic circumstances. You'd rather not go through the hassle of moving toward less dirigisme. It's so much easier to keep paying bribes.

The Central Intelligence Agency collects other economic intelligence, but the vast majority of it is not stolen secrets. The Aspin-Brown Commission four years ago found that about 95 % of US economic intelligence comes from open sources.

The Campbell report describes a sinister-sounding US meeting in Washington where — shudder! — CIA personnel are present and the participants — brace yourself — «identify major contracts open for bid» in Indonesia. Mr. Campbell, I suppose, imagines something like this: A crafty CIA spy steals stealthily out of a safe house, changes disguises, checks to make sure he's not under surveillance, coordinates with a spy satellite and ... buys an Indonesian newspaper. If you Europeans really think we go to such absurd lengths to obtain publicly available information, why don't you just laugh at us instead of getting in high dudgeon?

What are the economic secrets, in addition to bribery attempts, that we have conducted espionage to obtain? One example is some companies' efforts to conceal the transfer of dual-use technology. We follow sales of supercomputers and certain chemicals closely, because they can be used not only for commercial purposes but for the production of weapons of mass destruction. Another is economic activity in countries subject to sanctions — Serbian banking, Iraqi oil smuggling.

But do we collect or even sort secret intelligence for the benefit of specific American companies? Even Mr. Campbell admits that we don't, although he can't bring himself to say so except with a double negative: «In general this is not incorrect.» The Aspin-Brown Commission was more explicit:

«US Intelligence Agencies are not tasked to engage in 'industrial espionage' — i.e. obtaining trade secrets for the benefit of a US company or companies.»

The French government is forming a commission to look into all this. I hope the commissioners come to Washington. We should organize two seminars for them. One would cover our Foreign Corrupt Prac-

tices Act, and how we use it, quite effectively, to discourage US companies from bribing foreign governments. A second would cover why Adam Smith is a better guide than Colbert for 21 st-century economies. Then we could move on to industrial espionage, and our visitors could explain, if they can keep straight faces, that they don't engage in it. Will the next commission pursue the issue of rude American maitre d's?

Get serious, Europeans. Stop blaming us and reform your own statist economic policies. Then your companies can become more efficient and innovative, and they won't need to resort to bribery to compete.

And then we won't need to spy on you.

BIJLAGE 4

HOORZITTING MET DE BEGELEIDINGSCOMMISSIES VAN DE COMITES I EN P VAN DE SENAAT EN VAN DE KAMER VAN VOLKSVERTEGENWOORDIGERS — 15 JUNI 2001

Toepassing van de principes van de bescherming van de persoonlijke levenssfeer op het systeem «Echelon»

De Commissie voor de bescherming van de persoonlijke levenssfeer is bevoegd om vragen met betrekking tot de onderschepping van (tele)communicaties te onderzoeken in de mate dat krachtens de wet met betrekking tot de bescherming van de persoonlijke levenssfeer(1), gegevens met persoonlijk karakter behandeld worden, die betrekking hebben op fysiek geïdentificeerde of identificeerbare personen. De private telecommunicaties zijn beschermd door de voornoemde wet, maar eveneens door de wet met betrekking tot de bescherming van de persoonlijke levenssfeer tegen beluisteringen, kennisneming en opname van private communicaties en telecommunicaties(2), tegen elke kennisneming door een derde (enkel de partijen bij de communicatie zijn in staat het privaat karakter te bepalen).

In de loop van het jaar 1998 en op verzoek van de minister van Justitie, heeft de commissie de gelegenheid gehad zich te buigen over het bestaan en de werking van het systeem van onderschepping genoemd «Echelon». De commissie is in dit kader eveneens gecontacteerd door het Comité I, aan wie zij informatie heeft verschaft die toen voortvloeide uit de vooruitgang van haar onderzoek, alsook de namen van bepaalde experts (als die van Jean-Marc Dinant, informaticus bij de commissie en bij de Universitaire Faculteiten Notre-Dame de la Paix te Namen) die tenslotte bijgedragen hebben aan de redactie van het rapport(3) van het Comité R waarvan sprake zal zijn hierna.

Ten aanzien van de informatie waarover zij beschikte, heeft de commissie haar ongerustheid geuit aan de minister van Justitie wat betreft de eerbiediging van de bepalingen van nationaal recht inzake gegevensbescherming. Zij nam het initiatief tot een debat over de vraag te midden van de groep van artikel 29, die op Europees niveau de vertegenwoordigers van de verschillende nationale controleoverheden verantwoordelijk voor de bescherming van persoonsgegevens verzamelt. De officiële aanbeveling van de groep van artikel 29 van 3 mei 1999, aangehaald in het rapport van het Comité I, is aangenomen ten gevolge van deze debatten. De volledige tekst van deze aanbeveling is bijgevoegd aan het huidig document.

De bijzonderheden van de informatie vervat in het rapport van het Comité I bevestigen de uitgedrukte vrees op het nationaal niveau door de Commissie voor de bescherming van de persoonlijke levenssfeer, en op het Europees niveau door de groep van het artikel 29.

Het verslag bevestigt in het bijzonder dat «het zeker is dat het netwerk bestaat en belangrijke middelen bezit om heel het satelliet-verkeer ontvangen op het grondgebied van de Europese Unie af te luisteren».

(1) Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals gewijzigd door de wet van 11 december 1998, *Belgisch Staatsblad*, 3 februari 1999.

(2) Wet van 30 juni 1994, *Belgisch Staatsblad*, 24 januari 1995.

(3) «Aanvullend verslag over de wijze waarop de Belgische inlichtingendiensten reageren tegenover een mogelijkheid van een netwerk «Echelon» van onderschepping van communicaties», februari 2000.

ANNEXE 4

AUDITION PAR LES COMMISSIONS DU SUIVI DES COMITÉS R ET P DU SÉNAT ET DE LA CHAMBRE DES REPRÉSENTANTS — 15 JUIN 2001

Application des principes de protection de la vie privée au système «Echelon»

La Commission de la protection de la vie privée est compétente pour examiner les questions relatives à l'interception des (télé)communications dans la mesure où, aux termes de la loi relative à la protection de la vie privée(1), des données à caractère personnel sont traitées, qui sont relatives à des personnes physiques identifiées ou identifiables. Les télécommunications privées sont protégées par la loi précitée, mais également, par la loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées(2), contre toute prise de connaissance par un tiers à la communication (seules les parties à la communication sont à même de déterminer ce caractère privé).

Dans le courant de l'année 1998 et sur demande du ministre de la Justice, la commission a eu l'occasion de se pencher sur l'existence et le fonctionnement du système d'interception dénommé «Echelon». La commission a également dans ce contexte été contactée par le Comité R, à qui elle a fourni les éléments d'informations qui résultaient alors de l'avancement de son enquête, de même que les noms de certains experts (tels que celui de Jean-Marc Dinant, informaticien auprès de la commission et aux Facultés universitaires Notre-Dame de la Paix à Namur) qui ont en définitive contribué à la rédaction du rapport(3) du Comité R dont il sera question ci-après.

Au regard des informations dont elle disposait, la commission avait fait part au ministre de la Justice de ses inquiétudes quant au respect des dispositions de droit national en matière de protection des données. Elle prit l'initiative d'un débat sur la question au sein du groupe de l'article 29, qui rassemble au niveau européen les représentants des différentes autorités de contrôle nationales responsables de la protection des données à caractère personnel. La recommandation officielle du groupe de l'article 29 du 3 mai 1999, citée dans le rapport du Comité R, a été adoptée à la suite de ces débats. Le texte complet de cette recommandation est annexé au présent document.

Les détails des informations figurant dans le rapport du Comité R confirment les craintes exprimées au niveau national par la Commission de la protection de la vie privée, et au niveau européen par le groupe de l'article 29.

Le rapport affirme en particulier que «il est certain que [le] réseau (...) existe et possède des moyens importants d'écoute de tout le trafic satellitaire, reçu sur le territoire de l'Union européenne».

(1) Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, telle que modifiée par la loi du 11 décembre 1998, *Moniteur belge* du 3 février 1999.

(2) Loi du 30 juin 1994, *Moniteur belge*, 24 janvier 1995.

(3) «Rapport complémentaire sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau «Echelon» d'interception des communications», février 2000.

De besluiten verduidelijken nog dat «het evident is dat de Verenigde Staten en Groot-Brittannië over officiële diensten beschikken belast met het onderscheppen van telecommunicaties om veiligheidsredenen maar ook in het belang van het nationaal welzijn van de betrokken landen».

Het ontwerpverslag van het Europees Parlement «over het bestaan van een systeem van onderschepping van de hele wereld van private en economische communicaties (systeem van onderschepping Echelon)», bekendgemaakt op 18 mei 2001, mondt eveneens uit op het besluit volgens welk «het bestaan van een afluister-systeem van communicaties in werking, met de deelname van de Verenigde Staten, het Verenigd Koninkrijk, van Canada, van Australië en van Nieuw-Zeeland in het kader van het akkoord Ukusa, lijdt geen twijfel. Het is waarschijnlijk, ten opzichte van de beschikbare aanwijzingen, dat het Echelon genoemd wordt, maar dit aspect is van secundair belang. Wat telt is dat het gebruikt wordt om private en economische maar niet-militaire communicaties te onderscheppen» (1).

Wat ook het doel weze van de onderscheppingen (veiligheids- of economische aspecten), hun algemeen en verkennend karakter stoot op principes van zowel nationaal als internationaal recht, die zulk toezicht op grote schaal verbieden.

Het nationaal recht laat de verwerking van persoonsgegevens en in het bijzonder de onderschepping van telecommunicaties (elektronische post, telefoon, fax, ...) slechts toe binnen strikt bepaalde voorwaarden, en ten opzichte van een bepaald persoon.

Krachtens artikel 5 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, mogen deze gegevens niet overdreven zijn in verhouding tot het gevolgde doel.

Krachtens artikel 3 van de wet van 30 juni 1994 tot bescherming van de persoonlijke levenssfeer tegen afluistering, kennisneming en opname van private communicaties en telecommunicaties (2), is zulk een onderschepping slechts uitzonderlijk voorzien, door de onderzoeksrechter, zo er serieuze aanwijzingen bestaan van een inbreuk op de wet en als de andere onderzoeksmiddelen niet toelaten de waarheid te vinden.

Op Europees niveau gaat het algemeen en verkennend toezicht van de telecommunicaties in, in het bijzonder tegen de principes van het Europees verdrag tot bescherming van de mensenrechten en de fundamentele vrijheden van 4 november 1950 en de interpretatie van artikel 8 van het Verdrag door het Europees Hof van de rechten van de mens.

Het Europees Hof van de rechten van de mens (3) heeft gesteld dat een toezichtsysteem (4) artikel 8 van het Europees Verdrag tot bescherming van de mensenrechten eerbiedigt in de mate dat:

— de toezichtmaatregelen slechts kunnen uitgeoefend worden in het geval dat de aanwijzingen toelaten iemand te verdenken bepaalde ernstige inbreuken te plannen, uit te voeren of uitgevoerd te hebben;

— zij slechts kunnen voorgeschreven worden als de vaststelling van de feiten op een andere manier tot mislukken gedoemd is of ernstig gehinderd;

— het toezicht slechts betrekking heeft op de verdachte zelf of op de personen die vermoedelijk contacten hebben met hem.

Twee Europese richtlijnen bekrachtigen eveneens de verplichting tot bescherming van de persoonlijke levenssfeer en de ver-

Les conclusions précisent encore qu'il est évident que les États-Unis et la Grande-Bretagne disposent de services officiels (...) chargés d'intercepter des télécommunications à des fins de sécurité, mais aussi (...) dans l'intérêt du bien-être national des pays concernés».

Le projet de rapport du Parlement européen «sur l'existence d'un système d'interception mondial des communication privées et économiques (système d'interception Echelon)», rendu public le 18 mai 2001, aboutit également à la conclusion selon laquelle «l'existence d'un système d'écoute des communications fonctionnant, avec la participation des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande dans le cadre de l'accord Ukusa, ne fait plus de doute. Il est vraisemblable, eu égard aux indices disponibles, qu'il est dénommé Echelon, mais cet aspect est d'une importance secondaire. Ce qui compte, c'est qu'il est utilisé pour intercepter des communications privées et économiques mais non militaires» (1).

Quel que soit l'objectif des interceptions (aspects de sécurité ou économiques), leur caractère général et exploratoire se heurte aux principes tant de droit national qu'international, qui proscrivent une telle surveillance sur une grande échelle.

Le droit national ne permet le traitement de données à caractère personnel, et en particulier l'interception des télécommunications (courrier électronique, téléphone, fax, ...), que dans des conditions strictement définies, et à l'encontre d'une personne déterminée.

En vertu de l'article 5 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ces données ne peuvent être excessives par rapport à l'objectif poursuivi;

En vertu de l'article 3 de 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 (2), une telle interception n'est prévue qu'à titre exceptionnel, par le juge d'instruction, s'il existe des indices sérieux d'infraction à la loi et que les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

Au niveau européen, une surveillance générale et exploratoire des télécommunications va à l'encontre en particulier des principes de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et de l'interprétation de l'article 8 de la Convention par la Cour européenne des droits de l'homme.

La Cour européenne des droits de l'homme (3) a considéré qu'un système de surveillance (4) respecte l'article 8 de la Convention européenne de sauvegarde des droits de l'homme dans la mesure où:

— les mesures de surveillance ne peuvent être effectuées que dans les cas où des indices permettent de soupçonner quelqu'un de projeter, accomplir ou avoir accompli certaines infractions graves;

— elles ne peuvent être prescrites que si l'établissement des faits d'une autre manière est voué à l'échec ou considérablement entravé;

— la surveillance ne peut concerner que le suspect lui-même ou les personnes présumées avoir des contacts avec lui.

Deux directives européennes consacrent également l'obligation de protection de la vie privée et la confidentialité des communica-

---

(1) Tijdelijke Commissie over het systeem van onderschepping Echelon; rapporteur: Gerhard Schmid; PR/439868; http://www.europarl.eu.int/tempcom/echelon/prechelon-en.htm

(2) Dit artikel voegt artikel 90*ter* in het Wetboek van strafvordering.

(3) Arrest Klass, van 6 september 1978, serie A, nr. 28, blz. 23 en volgende.

(4) In dit geval het toezichtsysteem zoals uitgewerkt in het Duits recht.

(1) Commission temporaire su le système d'interception Echelon; rapporteur Gerhard Schmid; PR/439868; http://www.europarl.eu.int/tempcom/echelon/prechelon-en.htm.

(2) Cet article insère l'article 90*ter* dans le Code d'instruction criminelle.

(3) Arrêt Klass, du 6 septembre 1978, série A, n° 28, pp. 23 et suivantes.

(4) En l'occurrence le système de surveillance tel qu'élaboré en droit allemand.

trouwelijkheid van communicaties: de richtlijn 95/46/EG van 24 oktober 1995 met betrekking tot de bescherming van de fysieke personen ten opzichte van de verwerking van persoonsgegevens en van het vrije verkeer van deze gegevens, en de richtlijn 97/66/EG van 15 december 1997 met betrekking tot de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector van de telecommunicatie.

Het is van belang om op nationaal vlak zowel als op internationaal vlak en met eerbied voor deze teksten het nemen van maatregelen aan te moedigen met het oog op de versteviging van de veiligheid en de vertrouwelijkheid van de telecommunicaties.

Deze aanbeveling krijgt al zijn betekenis nu in het kader van de werken van de G8, de Raad van Europa en de Belgische Staat de inspanningen samen gaan bundelen om de onderschepping van telecommunicaties te vergemakkelijken met als doel de strijd tegen de informaticacriminaliteit.

Elk initiatief met het oog op het technisch toegankelijk maken van de inhoud en van de gegevens van telecommunicatie moet rekening houden met de bovenvermelde fundamentele principes en moet uitgevoerd worden in een transparant en een aan de nagestreefde doeleinden proportioneel kader.

De voorzitter,

P. Thomas

(1) Volgens artikel 13, paragraaf 1, van de richtlijn 95/46/EG, kan een lidstaat wetgevende maatregelen nemen met het oog op de beperking van de draagwijdte van bepaalde verplichtingen (bijvoorbeeld betreffende de inzameling van gegevens) en van bepaalde rechten (bijvoorbeeld het recht ingelicht te worden over een inzameling) voorzien door richtlijn 16. Deze uitzonderingen zijn strikt opgesomd: de beperking moet een noodzakelijke maatregel inhouden om de openbare belangen te vrijwaren op exhaustieve wijze opgesomd in de paragrafen *a)* tot *g)* van dit artikel, zoals de staatsveiligheid, defensie, de openbare veiligheid of de preventie, het zoeken de opsporing en de vervolging van strafrechtelijke inbreuken. In zijn artikel 14, paragraaf 1, bepaalt richtlijn 97/66/EG eveneens dat de lidstaten enkel de verplichting tot vertrouwelijkheid van de communicaties op publieke netwerken kunnen beperken als zulke maatregel noodzakelijk is voor de vrijwaring van de staatsveiligheid, defensie, de openbare veiligheid, de preventie, het zoeken, de opsporing en de vervolging van strafrechtelijke inbreuken.

tions: la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, et la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (1).

II importe qu'au niveau national comme au niveau international et dans le respect de ces textes, soit encouragée la prise de mesures visant à renforcer la sécurité et la confidentialité des télécommunications.

Cette recommandation prend tout son sens à l'heure actuelle, ainsi que, dans le cadre des travaux du G8, du Conseil de l'Europe et de l'État belge, les efforts convergent afin de faciliter l'interception des télécommunications dans le but de lutter contre la criminalité informatique.

Toute initiative visant à rendre techniquement accessibles le contenu et les données de télécommunications doit tenir compte des principes fondamentaux susmentionnés et être effectuée dans un cadre transparent et proportionnel aux objectifs poursuivis.

Le président,

P. Thomas.

(1) Selon l'article 13, § 1, de la directive 95/46/CE, un État membre peut prendre des mesures législatives visant à limiter la portée de certaines obligations (par exemple concernant la collecte de données) et de certains droits (par exemple le droit d'être informé sur une collecte) prévus par la directive 16. Ces exceptions sont strictement énumérées: la limitation doit constituer une mesure nécessaire pour sauvegarder les intérêts publics énoncés de façon exhaustive dans les paragraphes *a)* à *g)* de cet article, tels que la sûreté de l'Etat, la défense, la sécurité publique ou la prévention, la recherche, la détection et la poursuite d'infractions pénales. Dans son article 14, § 1, la directive 97/66/CE précise également que les États membres ne peuvent limiter l'obligation de confidentialité des communications sur des réseaux publics que lorsqu'une telle mesure constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales.

BIJLAGE 5

ANNEXE 5

GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

Aanbeveling 2/99 betreffende de bescherming van de persoonlijke levenssfeer in het kader van de interceptie van telecommunicatieverkeer. Goedgekeurd op 3 mei 1999

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS,

opgericht bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 (1),

gelet op de artikelen 29 en 30, leden 1 en 3, van voornoemde richtlijn (2),

gelet op haar reglement van orde, inzonderheid de artikelen 12 en 14,

heeft de volgende aanbeveling goedgekeurd:

De aanbeveling heeft tot doel eraan te herinneren dat de beginselen van bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, en met name van hun persoonlijke levenssfeer en het correspondentiegeheim, van toepassing zijn op de maatregelen die op Europees niveau op het gebied van interceptie van telecommunicatieverkeer zijn genomen.

Het toepassingsgebied van deze aanbeveling betreft interceptie in ruime zin, dat wil zeggen de interceptie van de inhoud van telecommunicatieverkeer, maar ook van de telecommunicatiegegevens, met name eventuele voorbereidende maatregelen (zoals «monitoring» en «datamining» van de verkeersgegevens) die zouden worden overwogen teneinde te kunnen beslissen over de wenselijkheid van de interceptie van de inhoud van het telecommunicatieverkeer (3).

A. Draagwijdte van de op Europees niveau goedgekeurde bepalingen inzake interceptie van telecommunicatieverkeer

1. De Resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer (4) bepaalt de

(1) Richtlijn van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PB* L 281 van 23.11.1995, blz. 31.

(2) De drie leden die respectievelijk de Registertilsynet (Denemarken) de Commission nationale de l'informatique et des libertés (CNIL, Frankrijk) en de Data Protection Registrar (Verenigd Koninkrijk) vertegenwoordigen, hebben niet aan de stemming over deze aanbeveling deelgenomen, daar zij van oordeel waren dat het behandelde thema niet tot de bevoegdheid van de Groep behoorde. Zij betuigen echter in het algemeen wel hun steun wat de grond van de aanbeveling betreft.

(3) Deze ruime betekenis van het begrip interceptie van telecommunicatieverkeer beantwoordt aan het toepassingsgebied van de Resolutie van de Raad van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer, die verder (punt A.1) wordt aangehaald, en aan het algemene kader van de terzake toepasselijke rechtsbepalingen (zie verder, punt B).

De aanbeveling is aldus van toepassing op de interceptie van niet-openbaar telecommunicatieverkeer op internet. De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens besteedt in het kader van werkzaamheden die parallel door de «Task force Internet» van de Groep worden uitgevoerd, bijzondere aandacht aan de algemene problematiek van de verwerking van persoonsgegevens die aan de ontwikkeling van Internet is verbonden.

(4) *PB* C 329 van 14.11.1996.

GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications. Adoptée le 3 mai 1999

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL,

Institué par la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 (1),

Considérant les articles 29 et 30, §§ 1 et 3, de la directive précitée (2),

Considérant son règlement intérieur, et en particulier les articles 12 et 14 de ce dernier,

À adopté la présente recommandation:

L'objectif de la recommandation est de rappeler l'application aux mesures adoptées au niveau européen en matière d'interception des télécommunications des principes de protection des droits et libertés fondamentaux des personnes physiques, et notamment de leur vie privée et du secret de la correspondance.

Le champ d'application de la présente recommandation vise les interceptions au sens large, c'est-à-dire l'interception du contenu des télécommunications mais également les données afférentes aux télécommunications, et notamment d'éventuelles mesures préparatoires (telles que «monitoring» et «datamining» des données de trafic) qui seraient envisagées afin de décider de l'opportunité de l'interception du contenu de la télécommunication (3).

A. Portée des dispositions adoptées au niveau européen en matière d'interception des communications

1. La résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (4) détaille les

(1) Directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *JO* L 281 du 23.11.1995, p. 31.

(2) Les trois membres représentant respectivement le Registertilsynet (Danemark), la Commission nationale de l'informatique et des libertés (CNIL, France) et le Data Protection Registrar (Royaume-Uni), n'ont pas participé au vote de cette recommandation, estimant que le sujet traité ne relevait pas de la compétence du groupe. Elles apportent néanmoins de façon générale leur soutien quant au fond de la recommandation.

(3) Ce caractère étendu de la notion d'interception des télécommunications correspond au champ d'application de la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, citée *infra* (Chapitre A.1), et au cadre général des dispositions juridiques applicables en la matière (voyez *infra*, chapitre B.).

La recommandation s'applique ainsi à l'interception des télécommunication non publiques sur internet. Une attention particulière est portée à la problématique générale du traitement de données personnelles liée au développement du réseau internet par le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dans le cadre de travaux menés parallèlement par la «task force internet» du groupe.

(4) *JO* C 329 du 14.11.1996.

noodzakelijke technische voorwaarden voor de interceptie van telecommunicatieverkeer, zonder dat wordt ingegaan op de vraag in welke omstandigheden deze interceptie zou moeten plaatsvinden. De tekst van de resolutie voorziet in een verplichting voor de netwerkexploitanten of de dienstenverstrekkers om de geïntercepteerde gegevens duidelijk aan de « wetshandhavingsdiensten » te verschaffen.

Deze gegevens betreffen telefoonoproepen, al of niet mobiel, elektronische post, fax- en telexberichten, de gegevensstroom op internet, zowel wat betreft de kennisneming van de inhoud van het telecommunicatieverkeer als van de telecommunicatiegegevens (deze betreffen met name de verkeersgegevens; maar ook elk signaal dat wordt uitgezonden door de persoon op wie de bewaking gericht is — punt 1.4.4 van de resolutie).

De gegevens hebben betrekking op de bewaakte persoon alsmede op de personen die deze persoon opbellen of door hem worden opgebeld (1).

De resolutie bepaalt ook dat de geografische locatie van de mobiele abonnee een gegeven is waartoe de wetshandhavingsdiensten toegang moeten kunnen krijgen (2).

Deze resolutie van 18 januari 1995 wordt momenteel herzien, voornamelijk om ze aan de nieuwe communicatietechnologieën aan te passen. De ontwerptekst voorziet met name in de toepassing van de interceptiemaatregelen op satellietcommunicatie (3).

2. De beschouwingen van de werkgroep hebben betrekking op het toepassingsgebied van de maatregelen waarin de Resolutie van de Raad van 17 januari 1995 voorziet. In een niet gepubliceerde en latere versie van voornoemd document (« intentieverklaring » van 25 oktober 1995) wordt bepaald dat de ondertekenaars van de tekst contact met de directeur van het « Federal Bureau of Investigation » van de Verenigde Staten zullen kunnen opnemen met betrekking tot de specificaties op het gebied van interceptie van telecommunicatieverkeer. In de tekst staat bovendien dat, mits de « deelnemers » daarmee instemmen, andere lidstaten kunnen deelnemen aan de uitwisseling van informatie, de herziening en de bijwerking van de specificaties.

De Groep wijst er enerzijds op dat de rechtsstatus van deze tekst — in het bijzonder de daadwerkelijke ondertekening door de betrokken landen — niet duidelijk is en dat het hier in de zin van de jurisprudentie van het Europees Hof voor de rechten van de mens niet gaat om een voor de burger toegankelijke maatregel, aangezien de tekst op geen enkele wijze is bekendgemaakt. Anderzijds wordt in deze tekst melding gemaakt van de wil om technische maatregelen inzake interceptie van telecommunicatieverkeer nader uit te werken in overleg met staten die niet zijn onderworpen aan de eisen van het Europees Verdrag tot bescherming van de rechten van de mens en de richtlijnen 95/46/EG en 97/66/EG.

3. De Groep constateert dat het de bedoeling is met de tekst van de resolutie van de Raad technische problemen te regelen met

(1) Artikel 1.4 van de bijlage bij de Resolutie van de Raad van 17 januari 1995.

(2) Artikel 1.5, *op. cit.*

(3) Document 10951/1/98, Enfopol 98 Rev 1 (http://www.heise.de/tp/deutsch/special/enfo/6332/l.html). Het schijnt dat een nog recentere versie door de Groep Politiële Samenwerking van de Raad is goedgekeurd en dat ze ter goedkeuring of wijziging aan het Europees Parlement is toegezonden. Blijkbaar is het de bedoeling de nieuwe resolutie op 27-28 mei 1999 door de Raad te laten goedkeuren (zie « Datenschutz-Berater », 15 februari 1999, blz. 5, waarin wordt verwezen naar een niet openbare versie van 20 januair 1999). De Commissie juridische zaken en rechten van de burger van het Europees Parlement heeft de Commissie openbare vrijheden en binnenlandse zaken (die in de eerste plaats bevoegd is) aanbevolen het ontwerp van herziening van de resolutie van de Raad zoals voorgesteld in Enfopol 98 af te wijzen, onder andere om redenen die verband houden met de bescherming van de persoonlijke levenssfeer en de aanstaande inwerkingtreding van het Verdrag van Amsterdam (zie verslag van de heer Florio). De Commissie openbare vrijheden heeft dit advies niet opgevolgd en zal de plenaire vergadering bijgevolg voorstellen Enfopol 98 op basis van het verslag van de heer Schmid goed te keuren. Het Europees Parlement zou begin mei zijn besluit moeten nemen.

conditions techniques nécessaires à l'interception des télécommunications, sans aborder la question des conditions dans lesquelles de telles interceptions devraient avoir lieu. Le texte de la résolution prévoit une obligation dans le chef des opérateurs de réseaux ou des fournisseurs de services de fournir en clair aux « services autorisés » les données interceptées.

Ces données visent les appels téléphoniques mobiles ou non, les courriers électroniques, les télécopies et messages télex, les flux de données internet, tant au niveau de la prise de connaissance du contenu des télécommunications que des données afférentes aux télécommunications (celles-ci se réfèrent notamment aux données de trafic, mais également à tout signal émis par la personne faisant l'objet la surveillance — point 1.4.4 de la résolution).

Les données concernent la personne surveillée ainsi que les personnes qui appellent ou qui sont appelées par cette personne (1).

La résolution prévoit également que la localisation géographique de l'utilisateur mobile constitue une donnée à laquelle les services autorisés doivent avoir accès (2).

Cette résolution du 18 janvier 1995 fait actuellement l'objet d'une révision, dont un des principaux objectifs est de s'adapter aux nouvelles technologies de communication. Le texte en projet précise en particulier l'application des mesures d'interception aux télécommunications par satellite (3).

2. Les réflexions du groupe de travail portent sur le champ d'application des mesures prévues par la résolution du Conseil du 17 janvier 1995. Une version non publiée du document précité et postérieure à celui-ci (« déclaration d'intention » en date du 25 octobre 1995), prévoit que les signataires du texte pourront prendre contact en ce qui concerne les spécifications en matière d'interception des télécommunications avec le directeur du « Federal Bureau of Investigation » des États-Unis. Le texte prévoit en outre que, sous réserve du consentement des « participants », d'autres États peuvent participer à l'échange d'informations, à la révision et à la mise à jour des spécifications.

Le groupe fait remarquer, d'une part, que le statut juridique de ce texte — en particulier sa signature effective par les pays concernés — n'est pas clair et qu'il ne constitue pas, au sens de la jurisprudence de la Cour européenne des droits de l'homme citée *infra*, une mesure accessible au citoyen dans la mesure où il ne fait l'objet d'aucune publication. D'autre part, ce texte fait état d'une volonté de mettre au point des mesures techniques d'interception des télécommunications en concertation avec des États non soumis aux exigences de la Convention européenne des droits de l'homme et des directives 95/46/CE et 97/66/CE.

3. Le groupe constate que le texte de la résolution du Conseil prétend régler des questions techniques relatives aux modalités

(1) Article 1.4 de l'annexe de la résolution du Conseil du 17 janvier 1995.

(2) Article I.5, *op. cit.*

(3) Document 10951/1/98, Enfopol 98 Rev 1 (http://www.heise.de/tp/deutsch/special/enfo/6332/1.html). Il semble qu'une version encore plus récente ait trouvé l'accord du groupe de travail « coopération policière » du Conseil et qu'elle ait été transmise au Parlement européen afin que celui-ci puisse l'adopter ou la modifier. Il est apparemment envisagé de faire adopter la nouvelle résolution par le Conseil les 27-28 mai 1999 (voyez « Datenschutz-Berater, 15.2.1999, p. 5, qui fait référence à une version non publique du 20.1.1999). La commission juridique et des droits des citoyens du Parlement européen a recommandé à la Commissions des libertés publiques et des affaires intérieures (chef de file) de rejeter le projet de révision de la recommandation du Conseil tel que proposé dans Enfopol 98 entre autres pour des raisons de protection de la vie privée et d'entrée en vigueur imminente du Traité d'Amsterdam (voir rapport de M. Florio). La Commission des libertés publiques n'a pas suivi cette avis et proposera donc à la plénière d'approuver Enfopol 98 sur base du rapport de M. Schmid. Le Parlement européen devrait prendre sa décision début mai.

betrekking tot de wijze waarop de interceptie van communicatie plaatsvindt, zonder dat de nationale bepalingen betreffende het aftappen van verbindingen uit juridisch oogpunt opnieuw worden bekeken. Nu blijkt echter dat sommige maatregelen waarin de resolutie voorziet en die tot doel hebben de mogelijkheden voor het intercepteren van communicatie uit te breiden, in strijd zijn met de nationale, meer beschermende, bepalingen van sommige landen van de Europese Unie (met name: punt 1.4, mededeling van de oproepgegevens, ook voor oproepen van mobiele abonnees, zonder dat rekening wordt gehouden met de momenteel beschikbare anonieme en vooruitbetaalde diensten; punt 1.5, geografische lokalisering van mobiele abonnees; punt 5.1, verbod voor de exploitanten om *a posteriori* bekend te maken welke intercepties zij hebben uitgevoerd).

4. Ofschoon met de resolutie van de Raad «de bescherming van het nationaal belang, de nationale veiligheid en de opheldering van zware misdrijven worden beoogd, wenst de Groep de aandacht te vestigen op de risico's van ontsporingen wat de doelstellingen van het aftappen betreft, risico's die nog zouden worden vergroot door uitbreiding van de technieken voor interceptie en decodering van telecommunicatieverkeer tot een steeds groter aantal landen — waarvan enkele buiten de Europese Unie.

In een officiële resolutie van 16 september 1998 over transatlantische betrekkingen(1) is het Europees Parlement «van oordeel dat het groeiende belang van internet en de wereldwijde telecommunicatie in het algemeen, met name het Echelon-systeem, alsmede de risico's die aan het misbruik daarvan zijn verbonden beschermende maatregelen vereisen op het terrein van economische informatie en een effectieve encryptie».

Met deze overwegingen wordt gewezen op de risico's die verbonden zijn aan de interceptie van telecommunicatieverkeer die verdergaat dan het strikte kader van aangelegenheden betreffende de nationale veiligheid — en aldus buiten het kader van de «derde pijler» van de Europese Unie valt. Daardoor rijst de vraag naar de legitimiteit ervan, met name in het licht van de verplichtingen die voor loeien uit de teksten van het Gemeenschapsrecht op het gebied van de bescherming van de grondrechten en fundamentele vrijheden van natuurlijke personen, en met name van hun persoonlijke levenssfeer.

5. Ten slotte wijst de Groep erop dat de inwerkingtreding van het Verdrag van Amsterdam zal leiden tot een verandering van de rechtsgrondslag op Europees niveau wat betreft de maatregelen inzake interceptie van telecommunicatieverkeer. In de huidige bevoegdheid van de Raad om de tekst van de resolutie op te stellen, die is gebaseerd op de artikelen K.1, lid 9, en K.3, lid 2, van het Verdrag, op het gebied van politiële en justitiële samenwerking, wordt op grond van het nieuwe artikel K.6, lid 2, plaats ingeruimd voor de initiatiefbevoegdheid van de Europese Commissie.

B. Algemeen rechtskader

6. De Groep herinnert eraan dat elke interceptie van telecommunicatieverkeer, waaronder wordt verstaan de kennisneming door een derde van de inhoud en/of de gegevens die op de private telecommunicatie tussen twee of meer correspondenten betrekking hebben, in het bijzonder de verkeersgegevens die aan het gebruik van telecommunicatiediensten verbonden zijn, een schending van het recht op persoonlijke levenssfeer en van het correspondentiegeheim vormt. Interceptie kan derhalve slechts worden

(1) Plenaire vergadering, notulen deel II, B4-0803, 0805, 0806 en 0809/98.

d'interception des communications, sans remettre en question les dispositions nationales réglementant les écoutes d'un point de vue juridique. Il s'avère cependant que certaines mesures prévues par la résolution et visant à élargir les possibilités d'interception des communications sont en contradiction avec les dispositions nationales, plus protectrices, de certains pays de l'Union européenne (notamment: point 1.4, communication des données afférentes aux appels y compris les appels des utilisateurs mobiles, sans qu'il soit tenu compte des services anonymes et prépayés actuellement disponibles; point 1.5, localisation géographique des utilisateurs mobiles; point 5.1, interdiction aux opérateurs de révéler *a posteriori* les interceptions qu'ils ont réalisées).

4. Si la résolution du Conseil s'inscrit dans un objectif de «protection des intérêts nationaux, de sécurité nationale et d'instruction en matière de criminalité grave», le groupe souhaite attirer l'attention sur les risques de dérives en ce qui concerne les objectifs des écoutes, risques qui seraient accrus par une extension à un nombre croissant de pays — extérieurs pour certains à l'Union européenne — des techniques d'interception et de décryptage des télécommunications.

Une résolution officielle du Parlement européen du 16 septembre 1998 relative aux relations transatlantiques(1), «estime que l'importance croissante du réseau internet, et plus généralement, des télécommunications à l'échelle mondiale et en particulier le système Echelon, ainsi que les risques de leur utilisation abusive, appellent l'adoption de mesures de protection des informations économiques et d'un cryptage efficace».

Ces considérations mettent en évidence les risques liés à une interception des télécommunications dépassant le cadre strict des questions de sécurité nationale — et sortant par là même du cadre du «troisième pilier» de l'Union européenne. Elles posent la question de leur légitimité notamment à la lumière des obligations découlant des textes de droit communautaire en matière de protection des droits et libertés fondamentaux des personnes physiques, et notamment de leur vie privée.

5. Le groupe souligne enfin que l'entrée en vigueur du Traité d'Amsterdam entraînera un changement de base juridique au niveau européen en ce qui concerne les mesures d'interception des télécommunications. La compétence actuelle du Conseil pour élaborer le texte de la résolution, basée sur les articles K.1(9) et K.3(2) du traité relatifs à la coopération policière et judiciaire, laissera place à une compétence d'initiative de la Commission européenne sur base de l'article K.6, § 2, nouveau.

B. Cadre juridique général

6. Le groupe rappelle que chaque interception de télécommunication, entendue comme la prise de connaissance par un tiers du contenu et/ou des données afférentes aux télécommunications privées entre deux ou plusieurs correspondants, en particulier les données de trafic liées à l'utilisation des services de télécommunication, constitue une violation du droit à la vie privée des individus et du secret de la correspondance. Une interception ne peut dès lors être admise que si elle répond à trois exigences fondamen-

(1) Session plénière, procès verbal partie II, B4-0803, 0805, 0806 et 0809/98.

toegestaan als zij voldoet aan drie fundamentele eisen overeenkomstig artikel 8, lid 2, van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden van 4 november 1950 (1) en de interpretatie die het Europees Hof voor de Rechten van de Mens aan deze bepaling heeft gegeven: een rechtsgrondslag, de noodzaak van de maatregel in een democratische maatschappij, en de beantwoording aan een van de legitieme doelstellingen die in het Verdrag worden vermeld (2).

In de rechtsgrondslag zal nauwkeurig moeten worden bepaald binnen welke grenzen en op welke wijze hij kan worden uitgeoefend, en dit door middel van duidelijke en gedetailleerde regels, die vooral noodzakelijk zijn omdat de bruikbare technische middelen voortdurend verder worden verbeterd (3). Deze wettekst moet voor het publiek toegankelijk zijn zodat de burger van tevoren weet welke gevolgen zijn gedrag zal hebben (4).

In deze juridische context moet de verkennende of algemene bewaking van telecommunicatieverkeer op grote schaal worden verboden (5).

7. In de Europese Unie huldigt Richtlijn 95/46/EG (6) het beginsel van de bescherming van het recht op persoonlijke le-

tales, conformément à l'article 8, § 2, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (1), et de l'interprétation réservée à cette disposition par la Cour européenne des droits de l'homme: une base légale, la nécessité de la mesure dans une société démocratique et la conformité à l'un des buts légitimes énumérés dans la convention (2).

La base légale devra définir précisément les limites et les modalités de son exercice, au moyen de règles claires et détaillées, qui sont surtout nécessaires en raison du perfectionnement continu des moyens techniques utilisables (3). Ce texte de loi doit être accessible au public afin que le citoyen puisse prévoir les conséquences de son comportement (4).

Dans ce contexte juridique, la surveillance exploratoire ou générale des télécommunications sur une grande échelle doit être proscrite (5).

7. Dans l'Union européenne, la directive 95/46/CE (6) consacre le principe de la protection du droit à la vie privée inscrit dans

---

(1) Er zij op gewezen dat de fundamentele waarborgen die door de Raad van Europa op het gebied van de interceptie van communicatie worden erkend, verplichtingen voor de staten scheppen, los van de verschillen die op het niveau van de Europese Unie bestaan naar gelang van het communautaire of intergouvernementele karakter van de beschouwde gebieden.

(2) Verdrag nr. 108 van de Raad van Europa bepaalt ook dat een maatregel tot inmenging slechts wordt toegestaan als het een maatregel betreft die in een democratische maatschappij noodzakelijk is voor de bescherming van de in artikel 9, lid 2, van dat verdrag opgesomde nationale belangen (hierbij zij opgemerkt dat de nationale belangen die in verdrag nr. 108 en in het Verdrag tot bescherming van de rechten de mens worden opgesomd, niet helemaal overeenstemmen), en als de maatregel strikt in liet licht van dit doel wordt gedefinieerd.

(3) Zie in dit verband, *infra*, de verplichtingen waarin wordt voorzien door artikel 4 van aanbeveling nr. 4 van de Raad van Europa betreffende de bescherming van persoonsgegevens op het gebied van telecommunicatiediensten, met name rekening houdend met telefoondiensten, van 7 februari 1995.

(4) Arresten-Huvig en -Kruslin tegen Frankrijk van 25 april 1990, serie A nr. 176 A en B, blz. 15 en volgende.

(5) Zie met name de arresten-Klass, van 6 september 1978, serie A nr. 28, blz 23 en volgende, en -Malone, van 2 augustus 1984, serie A nr. 82, blz. 30 en volgende.
In het arrest-Klass wordt, evenals in het arrest-Leander van 25 februari 1987, de nadruk gelegd op de noodzaak van «voldoende waarborgen tegen misbruiken, want een systeem van geheime bewaking ter bescherming van de nationale veiligheid houdt het risico in dat het, met de bedoeling de democratie te verdedigen, deze ondermijnt, en zelfs vernietigt» (arrest-Leander, serie A nr. 116, blz. 14 en volgende).
Het Hof merkt in het arrest-Klass (punt 50 en volgende) op dat de beoordeling van het bestaan van adequate en voldoende waarborgen tegen misbruiken afhangt van alle omstandigheden van de zaak. Het is in het desbetreffende arrest van oordeel dat de bewakingsmaatregelen waarin Duitse wetgeving voorziet, geen verkennende of algemene bewaking toestaan en geen inbreuk vormen op artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens. De Duitse wetgeving voorziet in de volgende waarborgen: de bewakingsmaatregelen kunnen slechts worden genomen in gevallen waarin iemand op grond van aanwijzingen ervan kan worden verdacht bepaalde ernstige overtredingen te beramen, te begaan of te hebben begaan; er kan slechts opdracht toe worden gegeven als het op een andere manier vaststellen van de feiten gedoemd is te mislukken of aanzienlijk wordt belemmerd; zelfs dan mag de bewaking alleen betrekking hebben op de verdachte zelf of de personen van wie wordt vermoed dat zij contact met hem onderhouden.

(6) Er zij op gewezen dat op grond van artikel 3 van Richtlijn 95/46/EG van het toepassingsgebied van de richtlijn zijn uitgesloten de verwerking van persoonsgegevens die met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten geschiedt alsmelde verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat, en de activiteiten van de Staat op strafrechtelijk gebied. De meeste lidstaten die deze richtlijn tot dusver hebben omgezet, maken in hun nationale wetten echter geen onderscheid volgens hetwelk deze wet niet van toepassing zou zijn op aangelegenheden die niet onder het Gemeenscliapsrecht vallen.
Daaraan wordt toegevoegd dat, wanneer de verwerking van gegevens in het kader van de richtlijn geschiedt (bijvoorbeeld lijst van oproepen die door een exploitant met het oog op facturering worden geregistreerd), maar deze gegevens naderhand het voorwerp uitmaken van een verwerking die in een interceptie van deze gegevens bestaat, de bepalingen van het Gemeenschapsrecht toepassing vinden. Richtlijn 95/46/EG voorziet in dit verband in een reeks waarborgen die bij deze intercepties in acht moeten worden genomen en waarop hierna nader wordt ingegaan.

---

(1) II convient de souligner que les garanties fondamentales reconnues par le Conseil de l'Europe en matière d'interception des communications engendrent des obligations à charge des États indépendamment des distinctions existant au niveau de l'Union européenne en fonction du caractère communautaire ou intergouvernemental des domaines abordés.

(2) La Convention nº 108 du Conseil de l'Europe prévoit également qu'une mesure d'ingérence n'est tolérée que lorsqu'elle constitue une mesure nécessaire dans une société démocratique à la protection des intérêts nationaux énumérés en son article 9, § 2, (on notera que les intérêts nationaux énumérés dans la convention 108 et dans la Convention de sauvegarde des droits de l'homme ne sont pas exactement similaires), et lorsqu'elle est strictement définie au regard de cette finalité.

(3) Voyez à ce sujet, *infra*, les obligations prévues par l'article 4 de la recommandation nº 4 du Conseil de l'Europe nº 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, du 7 février 1995.

(4) Arrêts Huvig et Kruslin contre France du 25 avril 1990, série A nº 176 A et B, pp. 15 et suivantes.

(5) Voyez notamment les arrêts Klass, du 6 septembre 1978, série A nº 28, pp. 23 et suivantes, et Malone, du 2 août 1984, série A nº 82, pp. 30 et suivantes.
L'arrêt Klass, comme l'arrêt Leander du 25 février 1987, insistent sur la nécessité de «garanties suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre» (arrêt Leander, série A, nº 116, pp. 14 et suivantes).
La Cour remarque dans l'arrêt Klass (§§ 50 et suivants) que l'appréciation de l'existence de garanties adéquates et suffisantes contre les abus dépend de toutes les circonstances de la cause. Elle considère dans l'arrêt en question que les mesures de surveillance prévues par la législation allemande n'autorisent pas la surveillance exploratoire ou générale et n'enfreignent pas l'article 8 de la Convention européenne de sauvegarde des droits de l'homme. Les garanties prévues par la loi allemande sont les suivantes: les mesures de surveillance ne peuvent être effectuées que dans les cas où des indices permettent de soupçonner quelqu'un de projeter, accomplir ou avoir accompli certaines infractions graves; elles ne peuvent être prescrite que si l'établissement des faits d'une autre manière est voué à l'échec ou considérablement entravé; même alors, la surveillance ne peut concerner que le suspect lui-même ou les personnes présumées avoir des contacts avec lui.

(6) On notera que l'article 3 de la directive 95/46/CE exclut de son champ d'application les traitements de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, et aux traitements ayant pour objet la sécurité publique, défense, la sûreté de l'État et les activités de l'État relatives à des domaines de droit pénal. La plupart des États membres ayant transposé cette directive jusqu'à présent n'opèrent toutefois pas, dans leurs lois nationales, une distinction selon laquelle cette loi ne s'appliquerait pas aux matières non couvertes par le droit communautaire.
On ajoute que, à partir du moment où un traitement de données est mis en œuvre dans le cadre de la directive (par exemple liste des appels enregistrès par un opérateur dans un objectif de facturation), mais fait dans un deuxième temps l'objet d'un traitement consistant en une interception de données, les dispositions de droit communautaire trouvent à s'appliquer. La directive 95/46/CE prévoit à cet égard une série de garanties devant être respectées dans le cadre de ces interceptions, qui sont développées ci-après.

venssfeer, dat in de rechtsstelsels van de lidstaten is vastgelegd. Deze richtlijn geeft een nadere omschrijving van de beginselen die zijn vervat in het Europees Verdrag tot bescherming van de rechten van de mens van 4 november 1950 en in het Verdrag van 28 januari 1981 van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens. Richtlijn 97/66/EG(1) concretiseert de bepalingen van deze richtlijn door aan de lidstaten de verplichting op te leggen het communicatiegeheim door middel van nationale reglementering te waarborgen en aldus het vertrouwelijk karakter te verzekeren van de communicatie die via een openbaar telecommunicatienetwerk of via algemeen beschikbare telecommunicatiediensten geschiedt.

Volgens artikel 13, lid 1, van Richtlijn 95/46/EG kan een lidstaat wettelijke maatregelen treffen ter beperking van de reikwijdte van bepaalde plichten (bijvoorbeeld betreffende het verzamelen van gegevens) en bepaalde rechten (bijvoorbeeld het recht om van het verzamelen van gegevens op de hoogte te worden gesteld) waarin de richtlijn voorziet(2). Er wordt een strikte opsomming van deze uitzonderingen gegeven: de beperking moet een noodzakelijke maatregel zijn ter vrijwaring van de openbare belangen die in de leden *a)* tot *g)* van dit artikel op exhaustieve wijze worden opgenoemd zoals de veiligheid van de staat, de landsverdediging, de openbare veiligheid of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

In artikel 14, lid 1, van Richtlijn 97/66/EG wordt ook bepaald dat de lidstaten de plicht tot het garanderen van het vertrouwelijk karakter van communicatie via openbare netwerken slechts kunnen beperken indien een dergelijke maatregel noodzakelijk is voor het vrijwaren van de veiligheid van de staat, de landsverdediging, de openbare veiligheid, alsmede voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

C. Verplichtingen van de telecommunicatie-exploitanten en de verstrekkers van telecommunicatiediensten

8. De nadruk moet worden gelegd op het feit dat de verplichtingen inzake beveiliging en vertrouwelijkheid van de gegevens waaraan de telecommunicatie-exploitanten, de dienstenverstrekkers, alsmede de lidstaten zijn onderworpen, respectievelijk op grond van de artikelen 17, leden 1 en 2, van Richtlijn 95/46/EG en de artikelen 4, 5 en 6 van Richtlijn 97/66/EG, het beginsel en niet de uitzondering vormen.

De Groep herinnert eraan dat deze verplichtingen in het algemeen ook gelden voor de exploitanten op grond van artikel 7 van Verdrag nr. 108 van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981, en van artikel 4 van aanbeveling nr. 4 van de Raad van Europa betreffende de bescher-

(1) Richtlijn van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *PB* L 24 van 30 januari 1998, blz. 1.

(2) Zoals bepaald in artikel 6, lid 1 — beginselen betreffende de kwaliteit van de gegevens, in artikel 10, artikel 11, lid 1 — informatieverstrekking aan de betrokkene, en in de artikelen 12 — rechts van toegang en 21 — openbaarheid van de verwerkingen.

les systèmes juridiques des États membres. Cette directive précise les principes contenus dans la Convention européenne de sauvegarde des droits de l'homme du 4 novembre 1950 et dans la Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La directive 97/66/CE(1) concrétise les dispositions de cette directive en précisant l'obligation incombant aux États membres de garantir le secret des communications au moyen de réglementations nationales durant la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessible au public.

Selon l'article 13, § 1, de la directive 95/46/CE, un État membre peut prendre des mesures législatives visant à limiter la portée de certaines obligations (par exemple concernant la collecte de données) et de certains droits (par exemple le droit d'être informé sur une collecte) prévus par la directive(2). Ces exceptions sont strictement énumérées: la limitation doit constituer une mesure nécessaire pour sauvegarder les intérêts publics énoncés de façon exhaustive dans les paragraphes *a)* à *g)* de cet article, tels que la sûreté de l'État, la défense, la sécurité publique ou la prévention, la recherche, la détection et la poursuite d'infractions pénales.

Dans son article 14, § 1, la directive 97/66/CE p'précise également que les États membres ne peuvent limiter l'obligation de confidentialité des communications sur des réseaux publics que lorsqu'une telle mesure constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique ou la prévention, la recherche, la détection et la poursuite d'infractions pénales.

C. Obligations des opérateurs et des fournisseurs de service de télécommunication

8. Il y a lieu d'insister sur le fait que les obligations de sécurité et de confidentialité des données auxquelles les opérateurs de télécommunication, les fournisseurs de services — ainsi que les États membres — sont soumis, respectivement sur base des articles 17, §§ 1 et 2, de la directive 95/46/CE et sur base des articles 4, 5 et 6 de la directive 97/66/CE, constituent le principe et non l'exception.

Le groupe rappelle que ces obligations s'imposent également de façon générale aux opérateurs en vertu de l'article 7 de la Convention du Conseil de l'Europe n° 108 pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981, et de l'article 4 de la recommandation du Conseil de l'Europe n° 4 sur la protection des données à caractère person-

(1) Directive du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, *JO* L 24 du 30 janvier 98, p .1.

(2) Prévu à l'article 6, paragraphe 1 — principes relatifs à la qualité des données, à l'article 10, à l'article 11, paragraphe 1 — information de la personne concernée, et aux articles 12. droit d'accès et 21 — publicité des traitements.

ming van persoonsgegevens op het gebied van telecommunicatiediensten, met name rekening houdend et telefoondiensten, van 7 februari 1995(1).

9. Deze verplichtingen impliceren enerzijds dat de telecommunicatie-exploitanten en de dienstenverstrekkers de gegevens betreffende het telelecommunicatie-verkeer en de facturering van de telecommunicatie slechts onder bepaalde voorwaarden kunnen verwerken: uit het beginsel dat de verkeersgegevens betreffende de abonnees en gebruikers moeten worden gewist of anoniem gemaakt zodra de communicatie is beëindigd, volgt dat de doeleinden waarvoor de gegevens kunnen worden verwerkt, de periode gedurende welke ze eventueel worden bewaard, alsmede de toegang tot de gegevens strikt beperkt zijn(2).

10. Anderzijds moeten de telecommunicatie-exploitanten en de verstrekkers van telecommunicatiediensten de nodige maatregelen treffen om de interceptie van telecommunicatieverkeer door niet bij wet daartoe gemachtigde instanties volgens de huidige stand van de techniek technisch moeilijk of onmogelijk te maken.

De Groep beklemtoont in dit verband dat het gebruik van doeltreffende middelen voor de interceptie van communicatie voor rechtmatige doeleinden, waarbij juist de meest geavanceerde technieken worden toegepast, niet mag leiden tot een verlaging van het algemene niveau van vertrouwelijkheid van de communicatie noch tot een vermindering van de bescherming van de persoonlijke levenssfeer.

Deze verplichtingen krijgen een bijzondere betekenis wanneer de telecommunicatie tussen personen die zich op het grondgebied van de lidstaten bevinden, een route volgt of kan volgen die gedeeltelijk buiten het Europese grondgebied ligt, met name bij het gebruik van satellieten of van internet.

11. Bovendien zou, in zoverre Richtlijn 95/46/EG van toepassing is, het toegankelijk maken van dergelijke telecommunicatie buiten de Europese Unie een schending van artikel 25 van de richtlijn kunnen zijn, aangezien de buitenlandse instanties die ze intercepteren, niet noodzakelijk een passend niveau van bescherming van de gegevens kunnen waarborgen.

nel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, du 7 février 1995(1).

9. Ces obligations impliquent, d'une part, que les opérateurs de télécommunication et les fournisseurs de services ne peuvent traiter les données relatives au trafic et à la facturation des télécommunications que selon certaines conditions: partant du principe que les données relatives au trafic concernant les abonnés et utilisateurs doivent être effacées ou rendu anonymes dès que la communication est terminée, il en suit que les finalités pour lesquelles les données peuvent être traitées, la durée de leurs conservation éventuelles ainsi que, l'accès aux données sont strictement limités(2).

10. D'autre part, les opérateurs de télécommunications et les fournisseurs de services de télécommunications doivent prendre les mesures nécessaires afin de rendre techniquement difficile ou impossible, selon l'état actuel de la technique, l'interception des télécommunications par des instances non autorisées par la loi.

Le groupe souligne à cet égard que la mise en œuvre de gens efficaces d'interception des communications à des fins légitimes, utilisant précisent les techniques les plus avancées, ne doit pas avoir pour conséquence d'abaisser le niveau général de confidentialité des communications et la protection de la vie privée des individus.

Ces obligations prennent un sens particulier dans le cas ou les télécommunications entre des personnes situées sur le territoire des États membres transitent ou peuvent transiter hors du territoire européen notamment lors de l'utilisation de satellites ou d'internet.

11. Dans la mesure où la directive 95/46/CE s'applique, le fait de rendre accessibles de telles télécommunications en dehors de l'Union européenne pourrait en outre constituer une violation de l'article 25 de la directive, étant donné que les instances étrangères qui les interceptent ne peuvent pas nécessairement prétendre assurer un niveau adéquat de protection aux données.

---

(1) «4.1. De door netwerkexploitanten of dienstenverstrekkers verzamelde en verwerkte persoonsgegevens mogen niet worden doorgegeven, tenzij de betrokken abonnee schriftelijk zijn uitdrukkelijke en geïnformeerde toestemming heeft verleend en de opgeroepen abonnees aan de hand van de verstrekte informatie niet kunnen worden geïdentificeerd.

De abonnee kan zijn toestemming op elk ogenblik intrekken, maar zonder terugwerkende kracht.

4.2. De door netwerkexploitanten of dienstenverstrekkers verzamelde en verwerkte persoonsgegevens mogen aan de overheid worden verstrekt als deze verstrekking bij wet is toegestaan en een maatregel is die in een democratische maatschappij noodzakelijk is voor:

a. de bescherming van de veiligheid van de Staat, de openbare veiligheid, de monetaire belangen van de Staat of de bestraffing van strafbare feiten

b. de bescherming van de betrokken persoon en van de rechten en vrijheden van anderen.

4.3. Bij de verstrekking van persoonsgegevens aan de overheid moet het nationale recht voorzien in de reglementering van:

a. de uitoefening van het recht op toegang en rectificatie door de betrokkene;

b. de voorwaarden waaronder de bevoegde overheidsorganen het recht hebben te weigeren inlichtingen aan de betrokkene te verstrekken of de afgifte ervan uit te stellen;

c. het bewaren en vernietigen van deze gegevens.»

(2) Zie met name de verplichtingen van artikel 6 van Richtlijn 97/66/EG.

Deze verplichtingen doen vragen rijzen met betrekking tot de praktijken die momenteel bij de verstrekkers van telecommunicatiediensten tot ontwikkeling komen en die bestaan in een algemeen en voorafgaand onderzoek van de verkeersgegevens van de abonnees, teneinde verdacht gedrag van bepaalde abonnees te constateren — en eventueel de gerichte interceptie van de inhoud van bepaald telecommunicatieverkeer mogelijk te maken.

(1) «4.1. Les données à caractère personnel collectées et traitées par les exploitants de réseau ou les fournisseurs de services ne devraient pas être communiquées, à moins que l'abonné concerné n'ait donné par écrit son consentement exprès et éclairé et que l'information communiquée ne permette pas d'identifier les abonnés appelés.

L'abonné peut retirer son consentement à tout moment mais de manière non rétroactive.

4.2. Les données à caractère personnel collectées et traitées par les exploitants de réseau ou les fournisseurs de services peuvent être communiquées aux autorités publiques si cette communication est prévue par la loi et constitue une mesure nécessaire, dans une société démocratique:

a. à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales;

b. à la protection de la personne concernée et des droits et libertés d'autrui.

4.3. En cas de communication de données à caractère personnel à des autorités publiques, le droit interne devrait réglementer:

a. l'exercice des droits d'accès et de rectification par la personne concernée;

b. les conditions dans lesquelles les autorités publiques compétentes seront en droit de refuser de donner des renseignements à la personne concernée ou d'en différer la délivrance;

c. la conservation ou la destruction de ces données.»

(2) Voyez en particulier les obligations de l'article 6 de la directive 97/66/CE.

Ces obligations suscitent des questions quant aux pratiques qui se développent actuellement parmi les prestataires de services de télécommunication et qui consistent en un examen général et préalable des données de trafic des abonnés, aux fins de repérer le comportement suspect de certains abonnés — et éventuellement de permettre l'interception ciblée du contenu de certaines télécommunications.

D. Eerbiedigingvandefundamentelevrijhedendoordeoverheid in het kader van interceptie

12. Het is belangrijk dat in het nationale recht met inachtneming van alle bovenvermelde bepalingen een zeer nauwkeurige omschrijving wordt gegeven van:

— de autoriteiten die bevoegd zijn om toestemming te geven tot de legale interceptie van telecommunicatie, de diensten die bevoegd zijn om de interceptie te verrichten, en de rechtsgrondslag voor hun optreden;

— de doeleinden waarvoor dergelijke intercepties kunnen worden uitgevoerd en aan de hand waarvan kan worden beoordeeld of ze in verhouding staan tot de nationale belangen die op het spel staan;

— het verbod van elke verkennende of algemene bewaking van telecommunicatieverkeer op grote schaal;

— de precieze omstandigheden en voorwaarden (bijvoorbeeld feitelijke elementen die de maatregel en de duur van de maatregel rechtvaardigen) waaronder de interceptie mag plaatsvinden, met inachtneming van het specificiteitsbeginsel dat op elke inmenging in het privé-leven van anderen van toepassing is (1);

— de inachtneming van dit specificiteitsbeginsel, een logisch gevolg van het verbod van elke verkennende of algemene bewaking, impliceert meer bepaald met betrekking tot verkeersgegevens dat de overheid slechts van geval tot geval, en niet op algemene en proactieve wijze, toegang tot deze gegevens kan krijgen;

— de beveiligingsmaatregelen wat de verwerking en de opslag van de gegevens betreft, alsmede de periode gedurende welke ze worden bewaard;

— met betrekking tot de indirect of toevallig bij het afluisteren betrokken personen (2), de bijzondere waarborgen die voor de verwerking van persoonsgegevens worden verstrekt: met name de criteria die het bewaren van de gegevens rechtvaardigen, en de voorwaarden waaronder deze gegevens aan derden kunnen worden verstrekt;

— de kennisgeving aan de bewaakte persoon, zodra dit mogelijk is (3),

— de vormen van beroep die de bewaakte persoon kan instellen (4),

— de wijze waarop een onafhankelijke controle-instantie toezicht op deze diensten uitoefent (5);

— de bekendmaking — bijvoorbeeld in de vorm van periodieke statistische verslagen — van het daadwerkelijk gevoerde beleid inzake interceptie van telecommunicatie (6);

(1) Zie *supra*, voetnoot 13.

(2) De hier bedoelde gegevens hebben betrekking op personen die zelf niet op bewakingsmaatregelen worden geviseerd, maar wel hun correspondent; bijvoorbeeld het door de bewaakt persoon gekozen telefoonnummer dat aan een verwant van hem toebehoort; de geografische lokalisering van bepaalde personen die per mobiele telefoon in contact staan met de afgeluisterde persoon.

(3) De onder bewaking geplaatste persoon zou immers op de hoogte moeten kunnen worden gebracht zodra de kennisgeving het onderzoek niet langer schaadt.

(4) In het voornoemde arrest-Leander wordt eraan herinnerd dat de instantie waarbij het beroep kan worden ingesteld «geen rechterlijke organisatie *strictu sensu* hoeft te zijn, maar dat haar bevoegdheden en de procedurewaarborgen die zij biedt, een rol spelen bij de beoordeling van de doeltreffendheid van het beroep». Onder dit beroep «moet worden verstaan een zo doelmatig mogelijk beroep, rekening houdend met de beperkingen die inherent zijn aan elk systeem voor geheime bewaking dat tot doel heeft de nationale veiligheid te beschermen» (§§ 83 en 84).

(5) Het arrest-Leander bedoelt de democratische controle op de intercepties wanneer het stelt dat «het de taak van het parlement en van onafhankelijke [overheids]instellingen is te waken voor het behoorlijke functioneren van het systeem» (§ 64).

(6) Deze eis tot bekendmaking alsmede, met name, de noodzaak van controle op de interceptie door een onafhankelijke instantie worden vermeld in het document «Common position public accountability in relation to interception of private communications» goedgekeurd in Hong Kong op 15 april 1998 door de internationale werkgroep inzake de bescherming van gegevens in de telecommunicatiesector.

D. Respectdeslibertésfondamentalesparlesautoritéspubliques dans le cadre des interceptions

12. Il importe que le droit national précise de façon rigoureuse et dans le respect de toutes les dispositions susmentionnées:

— les autorités habilitées à permettre l'interception légale des télécommunications, les services habilités à procéder aux interceptions et la base légale de leur intervention,

— les finalités selon lesquelles de telles interceptions peuvent avoir lieu, qui permettent d'apprécier leur proportionnalité au regard des intérêts nationaux en jeu,

— l'interdiction de toute surveillance exploratoire ou générale, des télécommunications sur une grande échelle,

— les circonstances et les conditions précises (par exemple éléments de fait justifiant la mesure, durée de la mesure) auxquelles sont soumises les'interceptions, dans le respect du principe de spécificité auquel est soumise toute ingérence dans la vie privée d'autrui (1),

— le respect de ce principe de spécificité, corollaire de l'interdiction de toute surveillance exploratoire ou générale, implique en ce qui concerne plus précisément les données de trafic que les autorités publiques ne peuvent avoir accès à ces données qu'au cas par cas, et non de façon générale et proactive,

— les mesures de sécurité en ce qui concerne le traitement et stockage des données, et leur durée de conservation,

— en ce qui concerne les personnes impliquées de façon indirecte ou aléatoire (2) dans les écoutes, les garanties particulières apportées au traitement des données à caractère personnel: notamment, les critères justifiant la conservations des données, et les conditions de la communication de ces données à des tiers,

— l'information de la personne surveillée, dès que possible (3),

— les types de recours que peut exercer la personne surveillée (4),

— les modalités de surveillance de ces services par une autorité contrôle indépendante (5),

— la publicité — par exemple sous forme de rapports statistiques réguliers — de la politique d'interception des télécommunications effectivement pratiquée (6),

(1) Voyez *supra*, note 13.

(2) Les données ici visées se rapportent à des personnes qui ne font pas l'objet de mesures de surveillance mais dont le correspondant fait l'objet de telles mesures; par exemple: numéro de téléphone composé par la personne surveillée et relatif à un parent de cette dernière; localisation géographique de certaines personnes en contact par téléphone mobile avec la personne sur écoute.

(3) La personne sous surveillance devrait en effet pouvoir être informée à partir du moment où l'information ne porte pas ou ne porte plus préjudice à l'investigation.

(4) L'arrêt Leander précité rappelle que l'instance devant laquelle le recours peut être exercé «n'a pas besoin d'être une institution judiciaire stricto sensu, mais que ses pouvoirs et les garanties de procédure dont elle s'entoure entrent en ligne de compte pour apprécier l'efficacité du recours». Ce recours «doit s'entendre d'un recours aussi effectif que possible, eu égard aux limitations inhérentes à tout système de surveillance secrète destiné à protéger la sécurité nationale» (§§ 83 et 84).

(5) L'arrêt Leander vise le contrôle démocratique des interceptions lorsqu'il précise que «c'est au Parlement et à des institutions indépendantes [du gouvernement] qu'il incombe de veiller à la bonne marche du système» (§ 64).

(6) Cette exigence de publicité, de même que, en particulier, la nécessité d'un contrôle des interceptions par une autorité indépendante, sont mentionnées dans la «Common position on public accountability in relation to interception of private communications» adoptée à Hong Kong le 15 avril 1998 par le groupe international de travail sur la protection des données dans le secteur des télécommunications.

— de precieze voorwaarden waaronder de gegevens in het kader van bi- of multilaterale overeenkomsten aan derden kunnen worden verstrekt.

Gedaan te Brussel, 3 mei 1999.

Voor de Groep,

De voorzitter

Peter HUSTINX.

— les conditions précises auxquelles les données peuvent être communiquées à des tiers dans le cadre d'accords bi- ou multilatéraux.

Fait à Bruxelles, le 3 mai 1999.

Par le Groupe,

Le président,

Peter HUSTINX.

BIJLAGE 6 | **ANNEXE 6**

L'EFFICACITÉ DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME POUR CONTESTER LE SYSTÈME «ECHELON»

Commission mixte Chambre-Sénat du suivi du Comité «R»

26 juin 2001

Assistant chargé de recherches
Centre de droit public
Université libre de Bruxelles

Dimitri YERNAULT

La présente communication écrite constitue une version mise à jour de celle qui a été présentée oralement le 22 mars 2001 devant la Commission temporaire du Parlement européen sur le réseau Echelon. Elle reprend pour l'essentiel, tout en les exposant différemment et en les actualisant, les arguments développés dans un article paru dans le numéro d'octobre 2000 du *Journal des Tribunaux-Droit Européen* («Echelon et l'Europe — La protection de la vie privée face à l'espionnage des communications») et dans une étude, actuellement sous presse, à paraître dans le numéro 2000-1 de la *Revue Belge de Droit International* («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»).

Les présents propos n'engagent bien évidemment que leur auteur.

1. LA CEDH N'INTERDIT PAS LES INTERCEPTIONS DE TÉLÉCOMMUNICATIONS MAIS ELLE LES ENCADRE

Depuis l'arrêt Klass contre Allemagne rendu en 1978, nous savons que la Cour européenne des droits de l'homme n'interdit pas les écoutes judiciaires, ni même les écoutes administratives. Mais les écoûtes, en ce qu'elles dérogent au principe du respect du droit à la vie privée et au respect de la correspondance porté par le § 1er de l'article 8 CEDH, doivent, conformément au § 2 de cette disposition, respecter trois conditions cumulatives.

Les trois conditions cumulatives de validité des interceptions de télécommunications sont, nous y reviendrons, le principe de légalité, le principe de légitimité et le principe de nécessité dans une société démocratique.

Il faut souligner que c'est en ayant bien à l'esprit les motifs tenant à ce qu'on pourrait appeler d'une formule ramassée la raison d'État, par exemple dans l'hypothèse qui nous occupe la sécurité nationale ou la protection du bien-être économique du pays, que les rédacteurs de la CEDH ont élaboré son article 8. La CEDH n'interdit pas les services de renseignement, elle s'en accommode même fort bien dès lors qu'ils visent à préserver l'ordre démocratique (arrêt Vereniging Weekblad Bluf! et arrêt Rotaru). Le fait est que la CEDH pose dans le même temps que sous peine d'instaurer un État policier, tous les moyens ne peuvent être utilisés sous prétexte de préserver cet ordre démocratique: tous les éléments essentiels de la jurisprudence sur les interceptions de télécommunications existent depuis ce fameux arrêt Klass de 1978.

Les États parties à la CEDH sont à ce point pleinement conscients de l'importance de celle-ci que le Royaume-Uni, pour ne prendre que cet exemple, a longuement justifié la compatibilité avec la CEDH (incorporée en 1998) du *Regulation of Investigatory Powers Act* 2000, loi qui régit désormais les pouvoirs d'interception du GCHQ. Le projet de réforme des services de renseignements analysé actuellement par le Parlement néerlandais se réclame également du respect de la CEDH.

2. LA VIE PRIVÉE DES CITOYENS DES PAYS PARTIES À L'ACCORD UKUSA EST, CENSÉMENT, PROTÉGÉE EN LEUR SEIN MAIS AU-DELÀ DE LEURS FRONTIÈRES?

En abordant le fond du problème, soit savoir comment protéger la vie privée à l'égard de systèmes transnationaux d'interception de télécommunications, force est de constater que les gouvernements et leurs services de renseignements assurent que la vie privée de leurs concitoyens est respectée.

Tel était le sens des exposés du lieutenant général Hayden, directeur de la NSA, et de George Tenet, directeur de la CIA, lors de leurs auditions du 12 avril 2000 par le House Select Committee on Intelligence: il s'agissait de rassurer les «US persons» pour lesquelles Constitution, législation et directives présidentielles prévoient une série de garanties. Le Congrès a donné quitus sur ce point aux agences de renseignement (Survey of activities of the Permanent Select Committee on Intelligence during the 106th Congress, Report HR 106-1054, 2 janvier 2001, p. 13).

Même souci manifestement du côté du directeur du DSD australien lorsqu'il reconnut en 1999 que son service collaborait sous les auspices de l'accord UKUSA avec d'autres pays (annexe 2 au rapport 1998-

1999 de l'Inspector-General of Intelligence and Security) : assurer les australiens que leurs services ne les écoutent pas (également le rapport 1999-2000 de l'IGIS).

Il est également très intéressant de lire ce type d'argumentaire dans le rapport 1999-2000 du commissaire du Centre de sécurité des télécommunications, l'agence SIGINT du Canada :

« (...) 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 États-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. Lorsqu'un pays fournit ainsi des signaux à un autre pays, on parle de collecte de renseignements par une seconde partie ».

Les gouvernements des pays qui participent à cet échange de renseignements ont des politiques destinées à protéger la vie privée de leurs citoyens. En particulier, chaque gouvernement a convenu de ne pas effectuer, pour le compte d'une seconde partie, de travail de collecte qui serait illégal dans le pays de cette seconde partie. Autrement dit, ils ne font pas indirectement ce qu'ils ne peuvent pas faire directement. »

Si l'on suit cette démonstration canadienne, identique à celle des autres pays censés former l'ossature d'Echelon ou participer à l'accord UKUSA, la vie privée de l'ensemble de leurs citoyens serait respectée par chacun d'entre eux aux termes d'accords croisés (voyez les doutes émis par Duncan Campbell dans la note distribuée lors de la séance du 22 mars 2001 de la Commission temporaire du Parlement européen). En admettant donc que ces législations nationales soient dûment appliquées, on peut difficilement conclure autre chose que celle-ci : les services de renseignement électronique des pays participant à UKUSA, Echelon ou tout autre système dirigent leurs appareils vers l'étranger, d'autres territoires, ... (adde sur la confirmation de la politique de renseignement avec les 4 autres pays anglo-saxons : *The Canadian Security and Intelligence Community, Government of Canada, Privy Council Office*, 2001, p. 17).

La confiance entre alliés (comme celle que, selon le rapport de Mr Paecht pour la mission d'information de l'Assemblée nationale française, manifesterait l'Allemagne à l'égard de la NSA qui ne tournerait pas les antennes de Bad Aibling contre les intérêts allemands) est une « garantie » qui paraîtra bien insuffisante aux autres États vers lesquels sont tournés les systèmes d'interception. Une situation en contrariété fondamentale avec un principe à la base même du droit international : la souveraineté territoriale. Une situation en contrariété fondamentale avec un droit imminent de la personne : l'intimité de la vie privée.

Parmi les documents officiellement existants, on compte également la décision Christie c. Royaume-Uni qui présente cet intérêt que, en 1994 déjà, le plaignant contestait la captation de fax échangés avec des syndicalistes polonais. Cette décision de l'ancienne Commission européenne des droits de l'homme s'est soldée par un rejet de la requête pour défaut manifeste de fondement aux termes d'une exceptionnellement longue analyse des garanties offertes par le droit anglais régissant les interceptions de télécommunications. Il faut toutefois savoir que l'établissement des faits de la cause faisait mention de l'éventuelle existence d'un « Dictionary » utilisé par le GCHQ pour capter toutes les communications entrant et sortant de Londres. Le *Dictionary* d'Echelon ? Peut-être. Mais, par delà cet indice troublant, la décision Christie montre l'aptitude des organes de la CEDH à traiter des dossiers comme celui d'Echelon.

3. LES RECOURS POSSIBLES ET LES MOYENS JURIDIQUES CONTRE LES INTERCEPTIONS TRANSFRONTALIÈRES : LA FORCE D'ATTRACTION DE LA CEDH

Plusieurs voies sont d'ores et déjà essayées : la plainte pénale contre X et/ou contre les États concernés (comme l'a fait l'eurodéputée allemande I. Schröder); l'enquête préliminaire du parquet (comme en France à la demande de l'eurodéputé français Th. Jean-Pierre); la plainte devant les juridictions de la résidence de ceux s'estimant victimes d'interceptions (plainte de l'association AKAWA devant le TGI de Paris). Il pourrait être envisagé aussi de se plaindre devant les juridictions d'un État du défaut de mesures prises par celui-ci pour protéger les télécommunications sur son territoire.

Mais il est tout aussi concevable qu'un État, pour autant qu'il estime que ses intérêts stratégiques, politiques et économiques ne s'y opposent pas, saisisse les juridictions internationales : la Cour internationale de justice pour violation de sa souveraineté territoriale ou le Comité des droits de l'homme de l'ONU en vertu de l'article 41 du Pacte international relatif aux droits civils et politiques pour violation de l'article 17 de celui-ci.

Un État européen pourrait surtout utilement saisir la Cour européenne des droits de l'homme, on revient toujours vers celle-ci (voyez la demande d'explications adressée par le sénateur Philippe Moureaux lors de la séance plénière du Sénat du 6 juillet 2000). L'arrêt Chypre contre Turquie du 10 mai 2001 rappelle à cet égard qu'un État est dans une situation plus favorable que les individus puisqu'il peut contester in abstracto les pratiques administratives ainsi que la législation d'un autre État signataire de la CEDH (infra le point sur le paradoxe juridique d'Echelon).

La mise en œuvre du mécanisme, traditionnel en droit international, de la protection diplomatique est une autre possibilité, notamment suggérée par la note du ministre de la Défense nationale des Pays-Bas du 19 janvier 2001.

Néanmoins, particuliers et Etats ne sont, juridiquement parlant, pas sur le même pied. Invoquer une violation de la souveraineté territoriale en contrariété avec l'article 2 de la Charte de l'ONU devant la Cour internationale de Justice est impossible pour les premiers.

Les individus ne peuvent de surcroît invoquer que des dispositions qui protègent effectivement leurs droits: la Déclaration universelle des droits de l'homme n'a, pour les États et donc pour les individus, aucune force juridique contraignante (c'est une simple résolution de l'AG de l'ONU). De même, l'article 22 de la Convention internationale des télécommunications (charte de l'UIT) n'engage ses États parties qu'à prendre toutes les mesures possibles pour garantir la confidentialité des télécommunications internationales. Cette Convention n'emporte donc pas d'effet direct pour les individus.

Par contre, deux dispositions peuvent être, *a priori*, invoqués par les individus se plaignant d'une violation de leur vie privée: l'article 17 du Pacte international relatif aux droits civils et politiques, d'une part, et l'article 8 CEDH, d'autre part.

Mais les possibilités de saisir, éventuellement, dans le premier cas le Comité des droits de l'homme de l'ONU sont singulièrement réduites, si l'on veut contester Echelon, puisque les USA et le Royaume-Uni n'ont pas adhéré au protocole facultatif permettant la saisine individuelle du Comité. Il serait tout aussi vain d'ailleurs de vouloir saisir les juridictions américaines puisque, comme l'ont montré les auditions des directeurs de la NSA et la CIA, les garanties constitutionnelles américaines ne sont pas applicables aux personnes «non américaines». Un des protagonistes supposés d'Echelon, et pas le moindre, ne peut donc pas être attaqué par un individu résidant ou ressortissant en Europe. On notera d'ailleurs que la proposition de résolution présentée devant la Commission temporaire du PE par son rapporteur, l'eurodéputé G. Schmidt, tend à inviter les USA à signer le protocole additionnel au PIDCP sans lequel les individus ne peuvent faire valoir leurs droits à l'encontre des USA devant le Comité des droits de l'homme (Projet de rapport sur l'existence d'un système d'interception mondial des communications privées et économiques — système d'interception Echelon —, 18 mai 2001, doc. PE 305.391, p. 13).

C'est donc en quelque sorte une nécessité juridique qui ramène vers la CEDH. Les USA n'y sont certes pas parties (ils ne semblent de toute façon pas pouvoir être attaqués) mais nous verrons que cette circonstance ne saurait absolument pas dispenser les États qui participeraient à Echelon et qui eux sont parties à la CEDH de respecter celle-ci. Même en étant le seul instrument international dont dispose les individus pour contester un système comme Echelon, la CEDH constitue de toute façon sans aucun doute l'instrument le plus apte à la défense des droits fondamentaux.

4. LA NATURE DE LA CEDH, TRAITÉ INTERNATIONAL GARANTISSANT «L'ORDRE PUBLIC EUROPÉEN» À ENVISAGER COMME UN ENSEMBLE COHÉRENT

Par delà la protection de la vie privée (l'article 8 CEDH inspirant de surcroît tout le droit du Conseil de l'Europe et de l'Union européenne) autour de laquelle un relatif consensus pourrait être formulé (par exemple la résolution du 11 avril 2000 de la Commission des libertés du Parlement européen), la chose la plus importante à avoir à l'esprit en ce qui concerne la CEDH, c'est bien qu'elle forme un ensemble cohérent forgé par 50 ans de jurisprudences strasbourgeoise et nationales. Force est de constater pourtant le grand nombre d'approximations concernant la protection effective qu'elle peut offrir à l'individu. Or, la CEDH régit incontestablement les rapports internationaux des États aussi, que ce soit à partir de leur territoire ou en raison du comportement de leurs organes déployant leurs effets en dehors du territoire.

• instrument de l'ordre public européen: tissu d'obligations objectives contractées par les États européens dans leurs relations entre eux mais aussi et d'abord à l'égard des particuliers sous leur juridiction (décision de la Commission de 1961 dans l'affaire Autriche contre Italie), la CEDH a été qualifiée en 1995 par la Cour de Strasbourg elle-même d'instrument de l'ordre public européen (arrêt sur les exceptions préliminaires dans l'affaire Loizidou contre Turquie). Ceci implique, comme l'a démontré un de ses plus brillants et renommés commentateurs, (F. Sudre, «Existe-t-il un ordre public européen?», in P. Tavernier (dir.), *Quelle Europe pour les droits de l'homme*, Bruxelles, Bruylant, 1996, p. 79) que «l'ordre public européen ne saurait s'accommoder de ce que ces valeurs puissent être méconnues sur le territoire d'un État partie, au motif que cette méconnaissance trouve sa source dans un jugement ou un acte étranger».

• un traité international: la CEDH est, on l'oublie trop souvent aussi, un traité, avec toutes les conséquences que cela implique en droit international. C'est un traité qui permet, tout à fait classiquement, la mise en ceuvre de la responsabilité internationale des États. C'est un traité qui ne régit jamais qu'une situation particulière mais laquelle!: la protection des droits fondamentaux. Les travaux des professeurs Condorelli, Dipla et Crawford (ce dernier est rapporteur spécial de la Commission du droit international de l'Assemblée générale de l'ONU sur la responsabilité internationale des États) ont ainsi particulièrement mis en avant les relations intimes, et la plupart du temps exceptionnellement novatrices, nouées entre le droit de la Convention et le droit de la responsabilité des États. À un point tel que le professeur Cohen-Jonathan estime que ce serait même plutôt la jurisprudence de la Cour EDH qui inspire bon nombre d'évolutions du droit de la responsabilité des États. L'interprétation actuelle de l'article 1er CEDH permet sans conteste d'établir la responsabilité des États qui

— soit participeraient activement à Echelon (ce qui serait le cas du Royaume-Uni), à partir de leur territoire ou en y faisant concourir leurs organes;

— soit participeraient passivement (ce qui serait plutôt le cas de l'Allemagne) en mettant leur territoire à disposition de services tiers.

• un traité international ayant donc une nature particulière: la CEDH présente cette importante particularité qu'en y adhérant, les États, en vertu de son article 53, reconnaissent sa primauté juridique sur toute autre norme internationale ou interne qui serait moins protectrice des droits fondamentaux portés par la Convention. Cette primauté a déjà été établie par la Cour européenne des droits de l'homme

dans des affaires nées de relations transfrontalières entre États parties et États non parties (le meilleur exemple, qui a servi de précédent, est sans conteste l'affaire Soering jugée en 1989 ou, en dernier lieu à propos des extraditions vers un État non partie à la CEDH où l'intéressé risque la torture, l'arrêt Hilal contre Royaume-Uni du 6 mars 2001) ou à propos de l'exécution du droit communautaire, même primaire comme le Traité de Maastricht, c'est-à-dire en raison des engagements noués par un État partie dans un ordre juridique tiers comme celui d'une organisation internationale (arrêt Matthews de 1999). Autrement dit, les faits, en contrariété ou même seulement potentiellement en contrariété avec la CEDH, qui trouvent leur source initiale dans le comportement d'un État complètement tiers à son espace de protection ne sauraient faire échapper à leur responsabilité propre au regard de la CEDH les États parties à celle-ci qui participent directement à sa violation par l'intermédiaire de leurs organes ou laissent se perpétrer des actes équivalant à violation faute de précautions suffisantes prises sur leur territoire.

5. LES CONDITIONS DU RESPECT DE L'ARTICLE 8

L'article 8 CEDH n'est pas seulement un précepte philosophique : c'est une règle concrète sous les auspices de laquelle l'intégralité du droit européen visant à la protection de la vie privée s'est en tous temps placé. Et lorsque l'on dit ici droit européen, il s'agit autant de l'ensemble des conventions, résolutions, recommandations et projets du Conseil de l'Europe que de l'arsenal juridique et politique déployé par les instances de l'Union européenne. Les articles 7 (respect de la vie privée, du domicile et des communications) et 8 (protection des données à caractère personnel) de la nouvelle Charte européenne des droits fondamentaux, approuvée lors du sommet de Nice, découlent directement de l'article 8 CEDH et de l'interprétation que lui donne la Cour européenne des droits de l'homme.

Les interceptions téléphoniques sont des actes de contrainte sur une volonté et donc des ingérences dans le droit au respect de la vie privée garanti par l'article 8 CEDH. Une telle affirmation ne constitue jamais que le rappel d'une jurisprudence constante de la Cour européenne des droits de l'homme, posée dès 1978 dans l'arrêt Klass contre Allemagne et soldée par la condamnation de trois pays différents en 2000 : la Suisse (arrêt Amman), la Roumanie (arrêt Rotaru) et le Royaume-Uni (arrêt Khan). Toute interception de communication, c'est-à-dire chaque forme quelconque de captation d'un message quelconque, est constitutive d'ingérence dans la vie privée au sens de l'article 8, § 1er, CEDH. Dès lors qu'il y a ingérence à la moindre interception, celle-ci ne peut passer pour valide au regard de l'article 8, § 2, CEDH que si elle répond à trois conditions cumulatives : la légalité, la légitimité et la nécessité dans une société démocratique.

1) La première, et pas la moindre, est la condition de légalité, laquelle impose plusieurs obligations :

• une « loi » doit exister pour permettre une ingérence. Le terme a une portée plus générale que celui de norme législative, la jurisprudence ou même des circulaires ministérielles peuvent en tenir lieu, ainsi qu'un traité international. Qu'une « loi » doive exister semble relever de l'évidence. Pourtant, l'arrêt A contre France condamna cette dernière en 1993 faute de toute réglementation sur l'interception querellée. Il en alla de même en 1997 dans l'arrêt Halford contre Royaume-Uni, ce qui justifia d'ailleurs l'adaptation de l'*Interception of Communications Act* de 1985 par le *Regulation of Investigatory Powers Act*. En admettant qu'existe bien l'accord Ukusa (ce qu'a reconnu un responsable australien), il est impossible de savoir à quel droit national applicable il renvoie. Echelon pose dès lors problème dès le tout premier stade de son analyse.

• une « loi », pour autant qu'elle existe, doit également être « accessible ». La contrariété d'Echelon avec l'article 8 CEDH ne fait alors vraiment plus aucun doute si, déclarations officielles recensées plus haut à l'appui, on veut bien se souvenir que :

+ la section 309 de l'*Intelligence Authorization Act 2000* adoptée par le Congrès américain visait précisément à connaître les bases légales des interceptions effectuées par la NSA et la CIA dans le cadre d'Echelon, d'une part, et si le contenu de certaines auditions par le Congrès est désormais connu, les résultats des délibérations du Congrès ne sont pas publiés, d'autre part;

+ un analyste australien a déclaré en août 1999 devant le Sénat australien que l'accord Ukusa, hautement classifié et dont on ne connaît que l'existence, était conservé dans un puits situé à Russel Hill;

+ le gouvernement britannique a officiellement répondu le 5 juin 2000 à une question parlementaire que les accords anglo-américains sur la gestion de la base de Menwith Hill étaient secrets, seul l'accord de 1951 sur le statut des troupes de l'OTAN étant disponible à la bibliothèque du Parlement.

Les Parlements d'États censés participer à Echelon ignorent ainsi eux-mêmes les accords internationaux régissant la manière d'opérer de leurs services de renseignement. Cela peut prêter à sourire. L'arrêt Rotaru contre Roumanie du 4 mai 2000 a estimé que la publication au *Journal Officiel* des normes applicables à la collecte de données personnelles par les services de renseignement suffisait à les rendre « accessibles ». Mais l'arrêt Khan du 12 mai 2000 a justement condamné le Royaume-Uni, à propos d'une interception policière menée dans le cadre d'un trafic de stupéfiants, parce que les circulaires du *Home Office* n'étaient pas publiées et seulement consultables à la bibliothèque du Parlement. Or, celle-ci ne contient même pas les accords secrets passés avec les services américains. Un citoyen britannique n'a déjà pas accès aux normes applicables. Que dire alors des citoyens des autres États ?

• la « loi » doit exister, être « accessible » mais également être « prévisible ». Ainsi le veut le principe de la prééminence du droit qui sous-tend toute la Convention, en particulier lorsque le pouvoir exécutif est

investi de larges pouvoirs discrétionnaires lui permettant de s'immiscer dans la vie privée d'un individu (arrêt Silver contre Royaume-Uni de 1984 à propos du contrôle de la correspondance des détenus). Faute d'assurance sur le degré d'intégration du pouvoir d'intercepter les communications téléphoniques dans des normes juridiques, le Royaume-Uni fut condamné en 1984 par l'arrêt Malone. Même si les mesures de surveillance secrètes justifiées par la sécurité nationale commandent un assouplissement de la condition d'accessibilité, il n'en demeure pas moins que toutes les personnes intéressées doivent connaître avec suffisamment de clarté les pratiques administratives gouvernant les enquêtes de sécurité (arrêt Leander contre Suède de 1987). Par conséquent, la France fut condamnée par les arrêts Huvig et Kruslin de 1990, l'Espagne par l'arrêt Valenzuela Contreras de 1998, la Suisse par les arrêts Kopp de 1998 et Amann de 2000, la Roumanie par l'arrêt Rotaru de 2000 également. À chaque fois dans des affaires d'écoutes téléphoniques. À chaque fois parce que les limites imposées au pouvoir d'interception par le droit interne étaient insuffisantes. Les mêmes principes s'appliquent à la conservation de données personnelles. Ils ont encore été rappelés dernièrement, à propos de la correspondance des détenus, dans l'arrêt Messina contre Italie du 28 septembre 2000.

• la «loi« doit exister, être «accessible», «prévisible» mais également respecter le droit international. Il ne sera pas revenu sur l'interdiction de principe formulée par le droit international général : même si un État peut conférer à sa législation une portée extra-territoriale, il ne peut conférer cette portée à actes matériels exécutifs. On oublie souvent aussi que pour être conforme à la CEDH, une ingérence doit respecter la «loi« (arrêt Barthold). Il est certain que la Cour européenne des droits de l'homme se refuse à se substituer aux juridictions nationales pour vérifier si un organe d'un État donné a appliqué correctement ou non le droit de cet État; c'est là la tâche du juge national. Il n'en demeure pas moins que la Cour, comme le Comité des droits de l'homme de l'ONU, se saisissent cependant de la conformité du comportement reproché au droit interne, donc à la «loi», dans les cas d'appréciation manifestement arbitraire ou de déni de justice flagrant (première application de cette exception dans l'arrêt Dulaurans contre France de 2000). Or la «loi» comporte également le droit international régulièrement en vigueur dans l'État concerné (arrêt Groppera Radio AG contre Suisse de 1990 à propos des conventions de l'Union internationale des télécommunications). Une violation flagrante du droit international ne saurait donc non plus mener à conclure que la «loi» a été respectée, surtout quand il s'agit d'un principe aussi éminent que celui du respect dû à la souveraineté territoriale des autres États qui est le fondement même du droit international, forgé par la coutume internationale et, notamment, exprimé par l'article 2 de la Charte de l'ONU. Il peut donc également être plaidé que les débordements territoriaux d'Echelon, non contents de violer le droit des gens, violent également l'article 8 CEDH qui impose que la «loi» soit respectée.

• la «loi» doit exister, être «accessible», «prévisible», respecter les fondamentaux du droit international mais aussi l'article 53 CEDH. Il a déjà été dit que l'article 53 consacre la primauté de la Convention sur toute autre norme interne ou internationale qui serait moins protectrice des droits de l'homme. La règle est également valable dans l'autre sens, c'est-à-dire que la Convention fait prévaloir la loi nationale si c'est celle-ci qui est plus protectrice des droits garantis. Le cas se présente notamment si l'on a égard au droit belge lequel, par définition, est le seul à avoir vocation à régir valablement les comportements sur le territoire belge. La Cour européenne des droits de l'homme admet les écoutes administratives, pour autant évidemment qu'elles se déroulent conformément à l'article 8. Mais le droit belge (sous réserve de deux exceptions, l'une très fortement critiquable également [article 295*bis*, § 5, du Code pénal autorisant les écoutes militaires à l'étranger par le Service général de renseignements de l'armée], l'autre pour des motifs purement techniques [article 109*ter*, D, de la loi du 21 mars 1991]) n'a nullement investi, pour l'heure, ses services de renseignement, ni aucun autre d'ailleurs, à procéder à des interceptions de télécommunications. Seules sont permises les écoutes effectuées sur mandat d'un juge d'instruction. Les écoûtes administratives, militaires, de sécurité, ... sont ainsi toujours prohibées sur le territoire belge. Pour une personne résidant sur celui-ci, il ne fait dès lors aucun doute que le droit belge est plus protecteur de la vie privée que la Convention elle-même et que le droit des États qui violent la souveraineté territoriale belge en y procédant à des actes d'interception. Une telle situation juridique ne se rencontre certes pas dans tous les États signataires de la CEDH mais là où elle existe, ne pas en tenir compte est tout autant de nature à violer l'article 8 CEDH !

2) Echelon peut donc être réputé violer l'article 8 CEDH alors même que celui-ci requiert que soient encore respectées, outre la condition de légalité, les conditions de légitimité et de nécessité dans une société démocratique. Une interception téléphonique ne sera légitime que si elle poursuit un des buts strictement énumérés par l'article 8, § 2. Le contrôle strasbourgeois est très limité en la matière mais affleure de plus en plus comme en atteste l'important opinion dissidente de plusieurs juges sous l'arrêt Rotaru qui se demandaient en quoi la conservation, sans discernement, d'informations sur la vie privée d'individus correspond à un souci légitime de sécurité nationale. De même que, contrairement à une opinion répandue, la CEDH protège les relations commerciales, le motif tiré de la préservation du bien-être économique d'un pays justifierait-il le contournement des règles de concurrence de l'OMC et de l'UE ? De même que, comme le rappelaient les principes directeurs de l'ONU de 1990 à propos des banques de données personnelles, on peut douter que la collecte systématique obéisse à des fins conformes aux principes de la Charte de l'ONU, ces fins fussent-elles de l'ordre de la sécurité nationale. La légitimité d'Echelon est pour le moins sujette à caution.

3) Par contre, la jurisprudence européenne relative à la troisième condition que doivent respecter les interceptions de télécommunications, à savoir celle de leur nécessité dans une société démocratique, est tout aussi substantielle que celle exposée à propos de la condition de légalité. Deux reproches majeurs peuvent être formulés à ce titre à l'égard d'Echelon : sa contrariété avec l'interdiction des écoutes exploratoires et générales, d'une part, et son déficit de garanties procédurales, d'autre part.

• Pour apprécier la nécessité des ingérences dans la vie privée, les États jouissent d'une marge d'appréciation, particulièrement large quand ils invoquent la préservation de leur sécurité nationale (celle-ci variant de pays à pays) mais qui pourrait l'être nettement moins quand il s'agit de la sauvegarde de leur bien-être économique (en raison du degré d'intégration internationale des réglementations de la concurrence). L'arrêt Klass contre Allemagne de 1978 a pourtant affirmé sans ambages que cette latitude n'était pas illimitée, sans quoi les mesures de surveillance secrète saperaient la démocratie au motif de la défendre. D'où l'interdiction des surveillances exploratoires et générales, selon l'expression de cet arrêt, interdiction dont la violation a été censurée à propos de la correspondance des détenus (arrêt Foxley contre Royaume-Uni de 2000) ou des perquisitions douanières (arrêt Miailhe contre France de 1993). Comme le dit l'Observation générale nº 16 du Comité des droits de l'homme de l'ONU, les écoutes ne peuvent intervenir qu'au cas par cas. C'est dès lors à bon droit que le groupe de travail « Article 29 » (Conférence des commissions nationales de protection de la vie privée, rattachée à la DG 15 de la Commission) fustige les systèmes généraux d'interceptions téléphoniques (document WP 18 du 3 mai 1999) ou le « sniffing », soit le contrôle généralisé du trafic des courriers électroniques (document WP 37 du 21 novembre 2000), pratiques en contrariété fondamentale avec l'article 8 CEDH. Faut-il préciser qu'étaient visés les systèmes Echelon et Carnivore ?

• La nouvelle dimension de l'article 8 CEDH au titre du contrôle de nécessité a trait à l'existence d'exigences procédurales : une ingérence n'est réputée proportionnée au but poursuivi que si elle intervient aux termes d'un processus décisionnel équitable pour l'individu. Ce principe s'applique aux perquisitions comme aux écoutes téléphoniques, administratives ou judiciaires. Dans le cas des écoutes administratives, il est au moins requis qu'existe un contrôle parlementaire suffisamment efficace (encore faut-il qu'il soit dûment accessible). Il faut admettre que c'est sur ce point que la jurisprudence de la Cour européenne des droits de l'homme reste la plus floue puisque les garanties procédurales sont parfois contrôlées dans le cadre de l'article 8, sous la condition de légalité mais aussi sous celle de nécessité, comme dans le cadre de l'article 13 CEDH qui porte le droit à un recours effectif. Mais il est en tout cas certain que des garanties minimales (par exemple sur la détermination des cibles, la durée de conservation des données et enregistrements, la notification de l'existence de l'interception, ...) doivent être respectées.

Il est important de souligner que l'ensemble de ces règles s'appliquent aux systèmes globaux d'interceptions, qu'ils puissent capter tout type ou seulement certains types de communications, mais aussi aux interceptions individualisées de cibles.

6. LA JURIDICTION DES ÉTATS PARTIES AU SENS D'ARTICLE 1er CEDH S'ÉTEND SUR TOUT LEUR TERRITOIRE MAIS AUSSI AU-DELÀ DE CELUI-CI

La jurisprudence de la Cour européenne des droits de l'homme s'inscrit pleinement, quand elle ne les anticipe pas, dans les nouvelles évolutions du droit des gens. Alors que les conséquences transfrontalières des comportements étatiques sont de plus en plus appréhendées par le droit international (notamment les autres travaux en cours de la CDI de l'ONU sur les pollutions transfrontalières), il est remarquable de constater que des règles de droit international nées à l'époque de l'impérialisme et du colonialisme les plus échevelés (voyez également les travaux en cours de la CDI de l'ONU sur la protection diplomatique), sont aujourd'hui le ferment de la contestation d'Échelon. On peut penser tout particulièrement aux obligations de prévention ou de diligence due initialement développées à propos de la protection des ressortissants étrangers sur le territoire d'un État tiers.

De telles obligations de vigilance ou de diligence due ne sont pas en voie de développement dans le cadre de la CEDH. Elles sont, et ce de longue date, la conséquence de l'économie et la philosophie inhérentes à la CEDH (théorie des obligations positives depuis l'arrêt Marckx contre Belgique de 1979). Ces obligations ont été consacrées à plusieurs reprises et à propos de plusieurs articles de la Convention.

La place de plus en plus accordée à l'article 13 CEDH (droit à un recours effectif devant une instance nationale pour contester les violations de la Convention) dans le système général de protection européenne des droits de l'homme permet d'ailleurs de contester désormais les violations structurelles des droits de l'homme et ce, à un moment où la jurisprudence relative aux conditions de recevabilité fait également l'objet d'assouplissements conséquents.

L'article 13 CEDH, comme les obligations positives inhérentes à la protection des autres droits garantis, a pour conséquence que les États ont le devoir de prévenir les violations quels qu'en soient les auteurs (organes de l'État, personnes privées, personnes internationales tierces) et, en cas de violations, d'enquêter, de punir celles-ci ainsi que, le cas échéant, de les réparer (notamment multitude d'affaires turques jugées depuis 1995 et, en dernier lieu l'arrêt Cicek contre Turquie du 27 février 2001 ou Berktay contre Turquie du 1er mars 2001).

Les obligations de vigilance ou de diligence due en matière de droits de l'homme ont été le mieux définies par la Cour interaméricaine des droits de l'homme, le 29 juillet 1988 dans l'arrêt Velasquez contre Honduras (§ 172). Un État doit veiller à la protection des droits de l'homme sur son territoire quels que soient les auteurs des violations commises : *« Il est clair qu'en principe est imputable à l'État 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 État 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 État — par exemple s'il est l'œuvre d'un particulier ou si son auteur n'est pas identifié — peut néanmoins engager la responsabi-*

lité internationale de l'État, non en raison du fait lui-même, mais en raison du manque de diligence de l'État pour prévenir la violation des droits de l'homme ou la traiter dans les termes requis par la Convention».

Un État peut donc être tenu pour responsable d'une violation de la CEDH s'il met son territoire à disposition d'un autre État, ce dernier perpétrant des actes équivalant à violation: c'est sa responsabilité propre que le premier État engage (hypothèse de l'accueil d'une station d'interception).

Du reste, un État demeure, on ne peut plus classiquement au regard du droit international, tenu des agissements de ses organes, y compris lorsque ceux-ci se déploient en dehors du territoire national (principe notamment rappelé dans les arrêts Drozd et Janouçek contre Espagne et France, Loizidou contre Turquie ou Chypre contre Turquie), ce qui sera le cas quand un service de renseignement électronique capte à partir du territoire national ou même d'un territoire tiers les communications se déroulant endehors du territoire national (hypothèse de la gestion d'une station d'interception).

Dans ces deux hypothèses, la primauté de la CEDH (*supra*, point 4) postule que l'État qui accueille une base et/ou en gère une lui-même reste tenu de ses actes propres, que ceux-ci soient menés par lui seul, en collaboration avec d'autres parties à la CEDH mais aussi en collaboration avec des pays non parties à la CEDH.

7. LE CAS DES INTERCEPTIONS TRANSFRONTALIÈRES DE COMMUNICATIONS: DROIT À LA VIE PRIVÉE ET SOUVERAINETÉ TERRITORIALE

La CEDH est donc un instrument juridique particulièrement adapté pour la protection des droits de l'homme, y compris dans les cas où c'est la manière dont un État mène ses relations internationales qui serait contestée. Les comportements des États parties qui ont des conséquences transfrontalières doivent eux aussi être conformes à la CEDH. Or, par-delà le respect dû à la souveraineté territoriale conformément au droit international général, un ensemble de textes, adoptés ou en préparation, traitent des interceptions transfrontalières de télécommunications, et du respect tout autant dû au droit à la vie privée. Cet ensemble de textes est d'importance:

• préambule de la résolution du Conseil européen du 17 janvier 1995 relative à l'interception légale des télécommunications (la fameuse résolution ENFOPOL affirmait quand même à raison que les interceptions doivent respecter la vie privée consacrée par les législations nationales territorialement applicables)

• recommandation n° R (95) 13 du 11 septembre 1995 du Comité des ministres du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information (nécessité du consentement des États en cas de perquisition informatique transfrontalière)

• projet de résolution de janvier 1999 de l'Institut de droit international sur les limites fixées par le droit international à la compétence des États sur les personnes relevant de leur juridiction (interdiction de l'acte de coercition, quel qu'il soit, transfrontalier à moins d'une autorisation préalable de l'État du for et possibilité pour les individus de pouvoir les contester [en particulier l'intervention de M. BEDJAOUI, juge à la CIJ, sur les possibilités offertes par l'article 1er CEDH à cet égard])

• rapport du 25 mars 1999 de Mr Schmid pour la Commission des libertés de votre Parlement (la résolution ENFOPOL de 1995, alors réévaluée, *«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»*)

• avis de la section de législation du Conseil d'État belge du 31 mai 1999 sur un projet de loi relatif à la criminalité informatique (rappel du principe de la souveraineté territoriale quant aux saisies informatiques transfrontalières, un État ne pouvant imposer à un autre, sans son consentement, une quelconque forme de coopération judiciaire internationale)

• résolution de la Commission des libertés du Parlement européen du 11 avril 2000 sur le système Échelon (rappel du principe de la notification de toute interception effectuée sur territoire étranger et des conditions du respect de l'article 8 CEDH)

• rapport explicatif du 30 novembre 2000 sur la convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (préservation intégrale des règles du droit international général en dehors des cas d'interception transfrontalière prévus par la Convention, soit uniquement les enquêtes pénales)

• 25e version du projet de Convention du Conseil de l'Europe sur la cybercriminalité, publiée le 9 janvier 2001 et notamment négociée avec les USA (suppression de la possibilité de pratiquer des interceptions transfrontalières; préambule et article 15 renvoyant au respect dû par ailleurs aux traités internationaux relatifs aux droits de l'homme)

• communication de la Commission européenne du 26 janvier 2001 pour Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité, COM (2001) 890 final, pp. 18-21 (visant explicitement Échelon et les interceptions abusives à l'échelle internationale comme contraires aux droits de l'homme)

• projet de rapport du 18 mai 2001 de Mr Schmidt pour la Commission temporaire sur le système Échelon du Parlement européen.

L'interdiction des interceptions transfrontalières en dehors du consentement de l'État (certains prônant la nécessité d'un accord préalable de celui-ci) où est localisée la cible ne constitue donc jamais qu'une application particulière d'un principe fondamental du droit international formulé en 1927 par la

Cour permanente de justice internationale dans l'affaire du Lotus : *« La limitation primordiale qu'impose le droit international à l'État est celle d'exercer, sauf l'existence d'une règle permissive contraire, tout exercice de sa puissance sur le territoire d'un autre État. Dans ce sens, la juridiction est certainement 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. »*

Un des exemples (ils sont très rares) de « règle permissive » est fourni par l'article 27 de la Convention de Vienne du 18 avril 1961 sur les relations diplomatiques et consulaires : l'État accréditaire permet et protège la libre communication de la mission pour toutes fins officielles mais son assentiment est indispensable pour l'installation et l'utilisation d'un poste de radio. Ces fins officielles doivent s'inscrire dans le cadre de l'article 3, § 1er : l'État accréditant protège ses intérêts et ceux de ses ressortissants sur le territoire de l'État accréditaire dans les limites admises par le droit international, d'une part, et si le premier peut s'informer et faire rapport sur l'évolution des événements dans le second, ce ne peut être qu'en utilisant des moyens licites, d'autre part. Hors ces conditions qui se placent à nouveau expressément sous l'empire du respect dû au droit international, un État ne peut donc théoriquement (c'est-à-dire juridiquement) pas rechercher autrement des informations, à plus forte raison sur un territoire autre que celui de l'État accréditaire.

Quand bien même, ce que semblent indiquer les réponses du Gouvernement britannique, la cogestion de la base de Menwith Hill se déroulerait-elle dans le cadre de l'Accord de Londres du 19 juin 1951 passé entre les États de l'OTAN sur le statut de leurs forces, l'article 2 de celui-ci impose le respect du droit de l'État d'accueil par les forces et les civils de l'État d'envoi, d'une part, et qu'ils s'abstiennent de toute activité contraire à l'esprit de l'Accord, d'autre part. Les gouvernements américain et britannique soutiendraient que les lois britanniques sur les interceptions de télécommunications sont respectées. Mais il faudrait alors objecter que le droit britannique doit respecter la CEDH également et que le gouvernement britannique ne pourrait se dédouaner unilatéralement des engagements y souscrits sous prétexte qu'il agit dans le cadre d'autres engagements internationaux. Sans rentrer dans les hypothèses complexes de responsabilité conjointe des États (la complicité est également appréhendée par les travaux de la Commission de droit international de l'ONU), il suffit ici de rappeler que les relations transfrontalières des États doivent s'inscrire dans le respect de leurs conventions particulières, du droit international général et, en ce qui concerne ceux qui sont parties à la CEDH, de celle-ci aussi, voire même avant toute autre règle internationale.

Le principe de souveraineté territoriale, tel que rappelé en 1927 dans l'Affaire du Lotus, reste la base même du droit international général. C'est si vrai que le Conseil européen, pour illustrer le propos dans un autre domaine, a décidé le 22 novembre 1996 une action commune relative aux mesures de protection contre les effets de l'application extra-territoriale d'une législation adoptée par un pays tiers (contestation des lois américaines dites D'Amato et Helms-Burton).

C'est si vrai aussi que le Conseil de l'Europe a supprimé la possibilité de recourir aux interceptions transfrontalières dans son projet de convention sur la cybercriminalité (la négociation ayant été notamment menée avec les USA) (sur les critiques toujours formulées au regard de l'article 8 CEDH notamment quant aux délais de conservation des données relatives au trafic, voyez l'avis 4/2001 du groupe de travail « Article 29 » sur la protection des données, doc. WP 41, ou X. Le Cerf, « Lutte contre la cybercriminalité : le projet de convention du Conseil de l'Europe contre la cybercriminalité », *Lex Electronica*, 2001, vol. 2).

Et si le Conseil des ministres UE a préservé la possibilité d'en pratiquer, il faut se souvenir que c'est contre l'avis du Parlement européen exprimé dans sa résolution législative du 17 février 2000. Le seul précédent international, publiquement, connu que constituent les articles 17 et suivants de la Convention sur l'entraide pénale montre bien de toute façon que les États membres de l'Union ne tolèrent les formes d'interception transfrontalières que dans un cadre conventionnel.

C'est exactement le même principe qui sous-tend celui de la sphère de sécurité (Safe Harbor) comme l'a montré, toute opinion étant réservée sur le fond, la décision de la Commission du 27 juillet 2000 autorisant, aux termes de longues négociations avec le Département américain du commerce, les transferts de données personnelles comme le requiert la directive 95/46/CE.

8. CONTESTER ECHELON DEVANT LA COUR EUROPÉENNE DES DROITS DE L'HOMME ?

La question primordiale reste, dans toutes ces hypothèses, avant tout celle de savoir s'il y a lieu ou non d'épuiser les voies de recours ménagées par le droit des États dont on soupçonne qu'ils font partie d'Echelon. Le droit international général requiert en principe l'épuisement préalable de ces recours. L'article 35 CEDH y renvoie d'ailleurs puisque le principe de l'épuisement a précisément pour objectif de préserver la souveraineté des États en leur permettant de redresser les situations dont il est allégué qu'elles violent les droits de l'homme. Or, ce principe connaît, en particulier dans l'ordre juridique généré par la CEDH, plusieurs exceptions dont trois au moins peuvent être invoquées pour ne pas épuiser les recours des États participant à Echelon.

• Ne doivent être épuisés que les recours internes qui sont effectifs, c'est-à-dire qui permettent de redresser la violation alléguée et accessibles. Prenons d'abord l'Allemagne qui se bornerait à accueillir sur son territoire une base de la NSA. La Cour a reconnu dans l'affaire Klass l'efficacité des modes de contrôle des interceptions de sécurité (dispositif connu sous le nom de « G 20 ») mais de celles effectuées par les services allemands. En supposant même que ces recours soient ouverts à des personnes ne résidant pas sur

le territoire allemand et qu'il puisse être passé outre à l'immunité de juridiction des services américains censément déployés dans le cadre des accords de 1951 sur l'OTAN, il semble établi que l'Allemagne, invoquant la confiance germano-américaine, ne contrôle pas si la NSA écoute ou non les citoyens et entreprises allemandes. On peut alors raisonnablement penser que l'Allemagne contrôle encore moins les activités de la NSA concernant des territoires nationaux tiers. Quelle serait de surcroît l'efficacité de recours dirigés contre un manquement à la CEDH par l'Allemagne qui trouve sa source première dans les agissements d'un service américain sous l'autorité d'un exécutif qui refuse de reconnaître ou démentir son implication dans Echelon ?

• Le même raisonnement peut être tenu à propos du Royaume-Uni en raison de son manque de vigilance sur son territoire à l'endroit des interceptions effectuées par la NSA. Le cas du Royaume-Uni présente toutefois cette singularité que cet État participe aussi aux interceptions comme l'établissent officiellement les réponses du Gouvernement à plusieurs questions parlementaires. Il peut alors sembler nécessaire d'épuiser les recours britanniques. Ceux-ci sont nombreux et les différentes législations applicables aux interceptions et aux services de renseignement ont été unifiées dans le RIPA 2000. Les travaux préparatoires de celui-ci insistent à satiété sur sa compatibilité avec le Human Rights Act de 1998 et le nombre de décisions de la Commission européenne des droits de l'homme qui ont conclu à la compatibilité avec la CEDH de ces législations (voir aussi les déclarations de l'ambassadeur de Grande-Bretagne en Belgique le 7 juillet 2000 après l'intervention de M. Moureaux au Sénat). Mais si l'on en croit le site Internet du MI 5 (les sites du GCHQ et du MI 6 ne comportent même pas de telles indications), le tribunal instauré par le Security Service Act de 1989 (qui sera remplacé par celui prévu par le RIPA) n'a, entre 1989 et 1997, retenu aucune des 275 plaintes introduites devant lui. Un recours voué à l'échec ne doit pas être épuisé selon la jurisprudence de la Cour européenne des droits de l'homme. Le refus du gouvernement de répondre à plusieurs questions parlementaires portant sur Echelon ou les réticences marquées par le Parlement britannique à répondre aux demandes formulées par d'autres missions d'enquête parlementaires nationales, voire de se déplacer devant votre commission, ne sont pas non plus de nature à forger la conviction de l'efficacité des recours britanniques, à plus forte raison si le plaignant ne réside pas sur le territoire britannique.

II n'est pas interdit non plus de se demander, Echelon étant supposé être un système multinational, quels sont les recours à épuiser : ceux de tous ou un seul État participant ? Si c'est d'un seul État lequel ? Ceux de tous les États ou seulement de ceux qui ont participé effectivement à l'interception querellée ? Que faire en cas de contrariété entre deux instances de recours l'une permettant l'accès aux données traitées, l'autre le refusant ? De toute façon, quand faut-il contester, la mesure de surveillance étant par essence secrète ? La NSA, le GCHQ notifient-ils à toutes les personnes dont une communication a été captée même si elle n'a pas fait l'objet d'un traitement ou d'un décryptage ? Au demeurant, l'éventuelle pluralité de recours à épuiser (soit ceux de plusieurs pays) soulèverait de sérieux problèmes puisque seules doivent être épuisés ceux organisés par des États parties à la CEDH (décision d'irrecevabilité du 19 juillet 2000, Luisa Diamantina Romero de Ibanez et Roberto Guillermo Rojas contre Royaume-Uni, requête nº 58692/00, communiqué de presse 542 de la Cour européenne des droits de l'homme).

Le fond (article 13 : droit à un recours effectif devant une instance nationale) et la procédure (article 35 : épuisement préalable des recours internes) sont intimement liés (par exemple les considérations de principe émises dans l'arrêt Aksoy contre Turquie en 1996). Il est douteux, à ce double égard, que les recours existants présentent le degré d'effectivité requis et qu'il faille donc les épuiser. Le refus (sauf de l'Australie) de reconnaître l'existence de l'accord UKUSA étaye cette thèse.

Pour achever de se convaincre de l'ineffectivité des recours « existants », on constatera d'abord que les voies de recours allemandes n'ont pas à être épuisées dès lors que l'Allemagne ne procède pas elle-même à des écoutes. Quant aux recours américains, ils ne doivent pas être épuisés non plus puisque les USA ne sont pas parties à la CEDH. Et ce, si l'on se place dans l'hypothèse d'un recours devant le Comité des droits de l'homme de l'ONU, quand bien même les USA viendraient à ratifier le protocole additionnel au PIDCP. En effet, la jurisprudence de la Cour suprême a dénié à un mexicain, lequel fit l'objet de perquisitions au Mexique à la suite d'opérations conjointes de la police mexicaine et de la DEA américaine, le bénéfice du 4e amendement de la Constitution américaine qui protège l'intégrité du domicile, et par extension celle de la vie privée. Cette disposition ne s'applique pas aux propriétés des étrangers non résidents et situées en territoire étranger [United States *versus* Yerdugo-Urquidez, 494 US 259 (1990)]. Il est dès lors parfaitement illusoire pour toute personne n'ayant pas la nationalité américaine et ne résidant pas sur le territoire américain d'attendre une quelconque protection du droit américain.

Pour ce qui est des recours britanniques, il faut enfin tenir compte de l'arrêt rendu le 20 juin 2000 par la Chambre des Lords dans l'affaire Holland *versus* Lamen-Wolfe qui, dans un simple litige social s'étant déroulé sur la base de Menwith Hill, a estimé que l'immunité de juridiction du gouvernement américain empêchait que celui-ci soit appelé à la cause devant les juridictions britanniques (un Lord a ajouté que les USA n'étant pas parties à la CEDH, la jurisprudence de la Cour sur les immunités ne pourrait pas leur être opposée). On peut se douter que dans des affaires où la sécurité nationale ne manquera pas d'être évoquée l'immunité de juridiction sera encore plus constitutive d'obstacle à l'effectivité des recours britanniques.

• En ce qui concerne les personnes résidant sur le territoire des États non participants à Echelon (ce qui constitue l'immense majorité des cas au sein du Conseil de l'Europe), il peut de surcroît être soutenu que la juridiction exercée par les services anglais en-dehors du territoire anglais est illicite au regard du droit international et, comme cela a été montré, de la CEDH. Cette juridiction internationalement illicite relève de l'obligation d'épuiser les voies de recours de l'État auteur de la violation d'un de ses engagements internationaux, en l'occurrence la CEDH. Cette juridiction internationalement illicite relève de

l'obligation d'épuiser les voies de recours de l'État auteur de la violation d'un de ses engagements internationaux, en l'occurrence la CEDH. C'est ce qu'a très concrètement décidé le 1er juillet 1999 le Tribunal international du droit de la Mer dans l'affaire du Saiga (arraisonnement douanier dans la zone économique exclusive alors que l'État côtier ne peut y procéder à des actes de contrainte). Même moins claires sur ce point, certaines décisions strasbourgeoises ont estimé que les recours turcs ne devaient pas, faute d'accessibilité et d'effectivité, être épuisés en cas de violation à Chypre des droits de l'homme des chypriotes par les forces armées turques (décision de recevabilité de l'ancienne Commission du 10 juillet 1978 dans une affaire Chypre contre Turquie) et que les recours à épuiser sont en principe ceux de son pays (arrêt Aksoy). Fond et procédure sont à nouveau intimement liés : l'illicéité d'un comportement contraire à la souveraineté territoriale entraîne en quelque sorte la « déchéance » pour l'État auteur du droit de se prévaloir du principe de l'épuisement.

Il faut cependant constater, même s'il a suscité d'importantes opinions dissidentes, que l'arrêt de la Cour européenne des droits de l'homme rendu ce 10 mai 2001 dans l'affaire Chypre contre Turquie a rejeté cette approche.

• Il peut de toute façon être plaidé que, même si elles sont conformes aux législations et circulaires des États participant à Echelon, les interceptions, dès lors qu'elles dépassent le cadre territorial permis par le droit international, n'en constituent pas moins des faits comme les autres au regard du droit des gens. Ces faits s'inscrivent dans un ensemble de violations semblables du droit à la vie privée, violations répétées et tolérées par les États concernés. Un tel ensemble de violations constitue des pratiques administratives. Celles-ci rendent vaine ou inefficace toute procédure parce qu'elles ne reposent sur aucun texte légale ou réglementaire qui puisse, en l'occurrence, être valablement excipé par les États membres d'Echelon. Les pratiques administratives étaient au Cour de l'arrêt Irlande contre Royaume-Uni de 1978 : leur existence dispensait d'épuiser les recours britanniques. Cette exception est parfaitement valable aussi en cas requête émanant de particuliers comme l'a posé l'arrêt Akdivar contre Turquie en 1996 qui définit les pratiques administratives comme « la répétition d'actes interdits par la Convention et la tolérance de l'État, de sorte que toute procédure serait vaine ou inefficace ». Echelon, dont la portée estimée concerne en tout cas la captation des communications par satellite, constitue en soi un tel ensemble de violations analogues et tolérées par les États qui y participent. Dénégations, semi-démentis et refus de collaboration des autorités en cause sont irrecevables, la tolérance étant disponible présumée dès qu'une pratique est suffisamment répandue. Dans ce cas également, il n'y a, ni pour un État, ni pour un particulier, obligation d'épuiser les recours allemands et britanniques.

L'arrêt Chypre contre Turquie vient de rappeler que l'existence de pratiques législatives et administratives en contrariété manifeste avec, notamment l'article 8 CEDH, dispense l'État requérant, mais également les particuliers qui s'en prévalent, de l'obligation d'épuiser les voies de recours internes ménagées par l'État défendeur. Et ce, à supposer même qu'elles existent et soient dûment accessibles, ce qui n'est pas le cas non plus. Cet important arrêt (en son § 297) admet surtout qu'une politique d'écoûtes téléphoniques systématiques d'une catégorie de la population puisse être constitutive de pratiques administratives.

9. LE PARADOXE JURIDIQUE D'ECHELON

L'arrêt Klass, toujours lui, en posant que « l'existence (...) de lois et pratiques autorisant et instaurant un système de surveillance secrète des communications constitue en soi une « ingérence », facilite considérablement la tâche de ceux qui désirent contester Echelon devant des juridictions internes ou européenne. C'est donc paradoxalement le caractère secret des systèmes de surveillance électronique qui offre ces facilités. Ce constat reste parfaitement valable sur le plan procédural. Un État qui voudrait saisir la Cour européenne des droits de l'homme n'a pas à démontrer d'un quelconque intérêt à agir, ce que commande le caractère objectif des obligations contractées en adhérant à la CEDH. Les particuliers (personnes physiques ou morales) doivent par contre démontrer qu'ils ont la qualité de victime en vertu de l'article 34 CEDH. Or, cette exigence est à nouveau singulièrement assouplie en cas de surveillance secrète : « 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 ». La qualité de victime « potentielle » a été consacrée dans les arrêts Klass de 1978, Malone de 1984 et Rotaru de 2000. La simple qualité d'usager des services de télécommunications suffit ainsi pour contester les atteintes directes aux droits garantis par l'article 8 de la CEDH que constituent les actes d'interception des télécommunications ! Plusieurs affaires anglaises dont a eu à connaître l'ancienne Commission européenne des droits de l'homme ont affirmé que le requérant n'avait pas à apporter la preuve de l'allégation selon laquelle les services de renseignements continuent à tenir des fichiers comportant des informations personnelles les concernant.

Le cas Echelon pose, pour ainsi dire, à son paroxysme les hypothèses d'interpénétration intime des aspects de fond et de procédure. C'est vrai en ce qui concerne l'efficacité des recours (articles 8 et 13 au fond et 35 sur le plan procédural). C'est vrai en ce qui concerne l'imputabilité à un État partie, question qui se situe aux confins de l'établissement des faits, d'une part, et de la compétence de la Cour européenne des droits de l'homme, d'autre part (article 1er). C'est vrai en ce qui concerne aussi l'existence d'une ingérence dans la vie privée, question de fond, et celle de la qualité de victime, question de procédure.

Même perfectibles, les moyens juridiques d'analyser et contrer d'ores et déjà Echelon, comme n'importe quel autre système similaire d'ailleurs, existent bel et bien.

La lutte contre les usages criminels des technologies des télécommunications est légitime mais elle doit aussi être licite. C'est ce que rappelait opportunément la résolution adoptée le 11 avril 2000 par la Commission des Libertés du Parlement européen.

Si l'on a pu regretter les approximations juridiques ayant affecté certains rapports parlementaires nationaux ainsi que les premiers travaux du Parlement européen au début de l'année 2000, la proposition de résolution en discussion au sein de la Commission temporaire du PE a désormais pris la juste mesure de la protection offerte à la vie privée par l'article 8 CEDH. En effet, le point 12 du projet de résolution «invite l'Allemagne et le Royaume-Uni à subordonner l'autorisation d'interception, sur leur territoire, de communications par les services de renseignements des États-Unis à la condition que cela se fasse dans le respect de la Convention relative aux droits de l'homme, c'est-à-dire conformément au principe de proportionnalité, que la base juridique soit accessible et que les effets soient prévisibles pour les personnes et qu'un contrôle efficace soit prévu, étant donné qu'ils sont responsables de la conformité avec les droits de l'homme des activités de renseignements autorisées ou tolérées sur leur territoire».

Cette position a été anticipée en 1999 par le groupe de travail «Article 29» rattaché à la DG 15 de la Commission européenne. Elle a été défendue devant la Commission parlementaire mixte Chambre-Sénat de suivi du Comité R par les professeurs Dinant et Poullet. L'auteur a eu l'honneur de la présenter devant la Commission temporaire du Parlement européen le 22 mars 2001, en même temps que M. R. Dossow, administrateur à la direction des médias du Conseil de l'Europe (dont la contribution a été remise en séance).

Ceci montre que tant le droit international général que le droit international et européen des droits de l'homme peuvent utilement protéger la vie privée des individus, sans préjudice des améliorations notamment proposées par la Commission temporaire du Parlement européen. Les principes portés en particulier par la CEDH n'ont pas seulement vocation à s'appliquer à Echelon. Ils concernent également tous les systèmes, nationaux ou internationaux, similaires. Ces principes, il convient de ne pas l'oublier, régissent d'abord la captation ciblée des communications d'individus, d'entreprises ou d'organisations non gouvernementales. Echelon n'est qu'une partie de l'iceberg. La surveillance de cibles déterminées au-delà des frontières d'un pays est techniquement parfaitement possible (une lettre du 27 avril 2000 de l'attorney general J. Reno indique que 880 requêtes ont été approuvées par la Foreign Intelligence Surveilance Court en 1999, laquelle n'a pas à intervenir pour la captation de cibles étrangères à l'étranger). Et les nouvelles technologies sont toujours plus performantes (l'existence du système TEMPEST, qui permet la captation des ondes émises par les écrans d'ordinateurs, est confirmée sur le site Internet du Communications — Electronics Security Group, une branche du GCHQ britannique. Sur d'autres systèmes: Th. Greene, «CIA patching ECHELON shortcomings», *The Register*, 6 mars 2001).

Face à la multiplication des dangers présentés par les nouvelles technologies de surveillance, la CEDH demeure l'instrument le plus efficace de protection des particuliers mais aussi des droits des États parties qui ont l'obligation de la respecter et de la faire respecter.

Indications bibliographiques:

• **P. Apraxine**, «Violation des droits de l'homme par une organisation internationale et responsabilité des États au regard de la Convention européenne des droits de l'homme», *Revue trimestrielle des droits de l'homme*, 1995, p. 27.

• **J. Barberis**, «Les liens juridiques entre l'État et son territoire: perspectives théoriques et évolution du droit international», *Annuaire français de droit international*, 1999, p. 132.

• **K. Boyle et H. Hannum**, «Individual applications under the European convention on human rights and the concept of administrative practice: the Donnelly case», *American journal of international law*, 1974, p. 440.

• **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, Cambridge University press, 1983.

• **G. Cohen-Jonathan**, «Les écoutes téléphoniques», in *Mélanges G.J. Wiarda*, Cologne, Karl Heymanns Verlag, 1988, p. 100; «L'arrêt Velasquez de la Cour interaméricaine des droits de l'homme», *Revue générale de droit international public*, 1990, p. 467; «La responsabilité pour atteinte aux droits de l'homme», in *La responsabilité dans le système international*, Paris, Pedone, 1991, p 101; «Les rapports entre la Convention européenne des droits de l'homme et les autres traités conclus par les États parties», in *Essays in the honour of HG Schermers*, III, Dordrecht, Martinus Nijhoff, 1993, p. 79; »Le rôle des principes généraux dans l'interprétation et l'application de la Convention européenne des droits de l'homme», in *Mélanges L.E. Pettiti*, Bruxelles, Bruylant, 1998, p. 172; *Aspects européens de la protection des droits fondamentaux*, 2e éd., Paris, Montchrestien, 1999; «Cour européenne des droits de l'homme et droit international général (1998-1999)», *Annuaire français de droit international*, 1999, p. 767.

• **L. Condorelli**, «L'imputation à l'État d'un fait internationalement illicite: solutions classiques et nouvelles tendances», *Recueil des cours de l'Académie de droit international*, 1984, VI, p. 154.

• **O. Corten et A. Schaus**, «La responsabilité internationale des États-Unis pour les dommages causés par les précipitations acides sur le territoire canadien», *Annuaire Canadien de Droit International*, 1989, p. 246.

• **V. Coussirat-Coustere**, «Convention européenne des droits de l'homme et droit interne: primauté et effets directs», in *La Convention européenne des droits de l'homme*, Bruxelles, Nemesis, 1992, p. 18; «Article 8 § 2», in L.E. Pettiti, E. Decaux et P.H. Imbert (dir.), *La Convention européenne des droits de l'homme — Commentaire article par article*, 2e tirage, Paris, Economica, 1999, p. 330.

• **J. Crawford**, *Premier rapport sur la responsabilité des États*, 50e session de la Commission du droit international de l'ONU, 1998, A/CN.4/490/Add.S; *Deuxième rapport sur la responsabilité internationale des États*, 51e session de la CDL, 1999, A/CN.4/498.

• **E. David et J. Salmon**, *Droit des gens*, tome II, 15e éd., Bruxelles, Presses Universitaires de Bruxelles, 1999-2000.

• **E. Decaux**, «Le territoire des droits de l'homme», in *Mélanges M.A. Eissen*, Bruxelles et Paris, Bruylant et Librairie générale de droit et de jurisprudence, 1995, p. 65.

• **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 nº 11*, Bruxelles, Bruylant et Nemesis, 1999, p. 57; «Le droit à un recours effectif», in *Mélanges P. Lambert*, Bruxelles, Bruylant, 2000, p. 188.

• **J. Dhommeaux**, «Les États parties à la Convention européenne des droits de l'homme et le Comité des droits de l'homme de l'ONU: 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 *Librairie générale de droit et de jurisprudence*, 1996, p. 119.

• **H. Dipla**, *La responsabilité de l'État pour violation des droits de l'homme — Problèmes d'imputation*, Paris, Pedone, 1994.

• **R. Dossow**, «The interception of communications and unauthorised acess to information stored on computer systems in the light of the European Convention on Human Rights», note distribuée lors de la séance publique du 22 mars 2001 de la Commission temporaire du Parlement européen sur le système Echelon.

• **J.R. Dugard**, *Premier rapport sur la protection diplomatique*, 52e session de la CDL, 2000, A/CN.4/506.

• **R. Ergec**, «Le contrôle juridictionnel des actes de l'administration dans les matières qui se rattâchent aux rapports internationaux: actes de gouvernement ou réserve de pouvoir discrétionnaire», *Revue de droit international et de droit comparé*, 1986, p. 131.

• **J.F. Flauss**, «Contentieux de la fonction publique internationale et Convention européenne des droits de l'homme» in *Études à la mémoire de J. Schwob*, Bruxelles, Bruylant, 1997, p. 161; «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*, Paris, Pedone, 1998, p. 24; «La Cour de Strasbourg face aux violations systématiques des droits de l'homme», in *Mélanges P. Lambert*, Bruxelles, Bruylant, 2000, p. 340.

• **W.J. Ganshof Van der Meersch**, «L'extradition et la Convention européenne des droits de l'homme», *Revue trimestrielle des droits de l'homme, 1990*, p. 22.

• **M.W. Janis**, «The Verdugo case: The United States and the Community of Nations», *European Journal of International Law*, 1991.

• **E. Kastanas**, *Unité et diversité: notions autonomes et marge d'appréciation des États dans la jurisprudence de la Cour européenne des droits de l'homme*, Bruylant, Bruxelles, 1996.

• **P. Klein**, *La responsabilité des organisations internationales dans les ordres juridiques internes et en droit des gens*, Bruxelles, Bruylant, 1998.

• **P. Lambert**, «Les bénéficiaires des droits de recours», in *La procédure devant la nouvelle Cour européenne des droits de l'homme après le Protocole nº 11*, Bruxelles, Bruylant et Nemesis, 1999, p. 16.

• **S. Marcus-Helmons**, «L'applicabilité de la Convention européenne des droits de l'homme aux personnes morales», *Journal des Tribunaux — Droit européen*, 1996, p. 151.

• **P. Mayer**, «La Convention européenne des droits de l'homme et l'application des normes étrangères», *Revue critique de droit international privé*, 1991, p. 651.

• **J.G. Merrills**, *The development of international law by the European court of human rights*, Manchester, Manchester University Press, 1988.

• **K.J. Park**, *La protection de la souveraineté aérienne*, Paris, Pedone, 1991.

• **A. Patijn**, «Data protection in the police sector», in *La protection des données dans le secteur de la police*, Strasbourg, Conseil de l'Europe, ADACS/DGI (2000) 3 Sem., p. 24.

• **E. Picard**, «Article 26», in L.E. Pettiti, E. Decaux et P.H. Imbert (dir.), *La Convention européenne des droits de l'homme — Commentaire article par article*, 2e tirage, Paris, Economica, 1999, p. 609.

• **P. Popelier**, «De openbaarheid van het overheidshandelen in het democratische rechtsstaat», *Tijdschrift voor bestuurswetenschappen en publiek recht*, 1995, p. 174.

• **N. Quoc Dinh, P. Dailler et A. Pellet**, *Droit international public*, 6e éd., Paris, Librairie générale de droit et de jurisprudence, 1999.

• **A. Reinisch**, «Widening the US Embargo against Cuba Extraterritoriality. A few Public International Law Comments on «Cuban Liberty and Democratic Solidarity Act 1996», *European Journal of International Law*, 1996.

• **J. Salmon et P. Klein**, *Responsabilité internationale*, tome I, Bruxelles, Presses universitaires de Bruxelles, 1998-1999.

• **C. Sciotti**, *La concurrence des traités relatifs aux droits de l'homme devant le juge national*, Bruxelles, Bruylant et Nemesis, 1997.

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

• **P. Sreenivasa Rao**, *Deuxième rapport sur la responsabilité internationale pour les conséquences préjudiciables découlant d'activités qui ne sont pas interdites par le droit international (prévention des dommages transfrontières résultant d'activités dangereuses)*, 51e session de la CDI de l'ONU, 1999, A/CN.4/501.

• **F. Sudre**, «Les obligations «positives» dans la jurisprudence européenne des droits de l'homme», *Revue trimestrielle des droits de l'homme*, 1995, p. 363; «Existe-t-il un ordre public européen?», in P. Tavernier (dir.), *Quelle Europe pour les droits de l'homme?*, Bruxelles, Bruylant, 1996, p. 39; (dir.), *L'interprétation de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant et Nemesis, 1998; *Droit international et européen des droits de l'homme*, 4e éd., Paris, Presses universitaires de France, 1999.

• **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, Bruylant, 1996, p. 17.

• **H. Tigroudja**, «L'immunité de juridiction des organisations internationales et le droit d'accès à un tribunal», *Revue trimestrielle des droits de l'homme*, 2000, p. 101.

• **J. Verhoeven**, *Droit international public*, Bruxelles, Larcier, 2000.

• **P. Waschmann**, «Les écoutes téléphoniques», obs. sous l'arrêt A. c. France du 23 novembre 1993, *Revue Trimestrielle des droits de l'homme*, 1994, p. 582; «La prééminence du droit dans la jurisprudence de la Cour européenne des droits de l'homme», in *Études en l'honneur de J. Schwob*, Bruxelles, Bruylant, 1997, p. 241.

• **L. Weitzel**, «La Commission européenne des droits de l'homme et le droit communautaire», in *Mélanges J. Velu*, III, Bruxelles, Bruylant, 1992, p. 1391.

• **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 des droits de l'homme», *Revue trimestrielle des droits de l'homme*, 1994, p. 121; «Libertés classiques et droits dérivés: le cas de l'accès aux documents administratifs», *Revue trimestrielle des droits de l'homme*, 1996, p 225; «Echelon et l'Europe: la protection de la vie privée face à l'espionnage des communications», *Journal des Tribunaux Droit européen*, octobre 2000, p. 187.

• XXX, «Computers and International Criminal Law: High Tech Crimes and Criminals», *New England International and Comparative Lawx Annual*, 2000, p. 110 (nom de l'auteur non retrouvé).

59.835 — E. Guyot, n. v., Brussel