Annotation: EHRM 2008-07-01

Groothuis, M.M.

ONDERSCHEPPEN VAN TELEFOON- EN E-MAILVERKEER: EIS VAN VOORZIENBAARHEID BIJ WET

Europees Hof voor de Rechten van de Mens 1 juli 2008, Liberty t. Verenigd Koninkrijk (appl. no. 58243/00) *

Met noot van Marga Groothuis **

In het Verenigd Koninkrijk wordt het telefoon-, e-mail en dataverkeer onderschept met een schotel van het ministerie van Defensie. Drie mensenrechtenorganisaties dienen een klacht in over deze onderschepping. Het Hof overweegt dat het, in de context van het onderscheppen en afluisteren van communicatie, essentieel is dat er duidelijke en gedetailleerde regelgeving is. Aldus wordt aan burgers duidelijk onder welke omstandigheden en voorwaarden de autoriteiten zijn gemachtigd om zulke bevoegdheden jegens hen te gebruiken. Het Hof oordeelt dat het Britse rechtssysteem niet in voldoende duidelijke mate de reikwijdte en randvoorwaarden voor de afluisterbevoegdheden formuleert en dat de inbreuk op de rechten van de klagers onder art. 8 EVRM derhalve niet voldoet aan de eis van voorzienbaarheid bij wet.

FEITEN EN RECHTSGANG OP NATIONAAL NIVEAU

De klagers in deze zaak zijn Liberty, British Irish Rights Watch en de Irish Council for Civil Liberties, een Britse en twee Ierse mensenrechtenorganisaties gevestigd in respectievelijk Londen en Dublin. De zaak betreft hun klacht dat tussen 1990 en 1997 hun telefoon-, e-mail- en dataverkeer, inclusief vertrouwelijke informatie, werd onderschept door een zogeheten Electronic Test Facility, een schotel voor het onderscheppen van telecommunicatie, die werd gebruikt door het Britse ministerie van Defensie.

Deze schotel (verder: ETF), die was opgesteld in Capenhurst, Cheshire, was gebouwd met het doel om 10.000 parallelle telefoonkanalen tussen Dublin en Londen en tussen Londen en het continent te kunnen afluisteren. De klagers stelden dat de ETF van 1990 tot 1997 alle via twee centrale stations van British Telecom (in Clwyd en Chester) gevoerde publieke communicatie, inclusief alle telefoongesprekken en e-mailberichten, onderschepte. Gedurende deze periode onderhielden de klagers regelmatig telefonisch contact met elkaar en boden zij onder meer juridisch advies aan personen die hulp bij hen zochten. Zij stelden dat een groot deel van hun communicatieverkeer via de twee stations van British Telecom was getransporteerd en aldus zou zijn onderschept door de ETF.

In 1999 dienden de drie mensenrechtenorganisaties klachten over deze onderschepping van hun communicatie in bij de *Interception of Communications Tribunal*, bij de hoofdofficier van justitie en bij de *Investigatory Powers Tribunal*, stellende dat deze onderschepping onrechtmatig was, meer in het bijzonder in strijd met de Britse Wet op de Onderschepping van Communicatie 1985. Hun klachten werden door elk van deze instanties verworpen.

* Samenstelling Hof: Garlicki (Pres.), Bratza, Mijović, Björgvinsson, Šikuta, Hirvelä, Poalelungi.

** Mr. M.M. Groothuis is universitair docent staats- en bestuursrecht aan de Universiteit Leiden.

HET ARREST VAN HET EHRM

Het EHRM overweegt als volgt:

'(...)
THE LAW
I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION
41. The applicants complained about the interception of their communications, contrary to Article 8 of the Convention:
'1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

A. The parties' submissions
1. The applicants
42. The applicants complained that, between 1990 and 1997, telephone, facsimile, e-mail and data communications between them were intercepted by the Capenhurst facility, including legally privileged and confidential material.
43. Through the statements of Mr Duncan Campbell, a telecommunications expert, they alleged that the process applying to external warrants under section 3(2) of the 1985 Act embodied five stages.
First, a warrant would be issued, specifying an external communications link or links to be physically intercepted. Such warrants covered very broad classes of communications, for example, 'all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe'. All communications falling within the specified category would be physically intercepted.
Secondly, the Secretary of State would issue a certificate, describing the categories of information which could be extracted from the total volume of communications intercepted under a particular warrant. Certificates were formulated in general terms, and related only to intelligence tasks and priorities; they did not identify specific targets or addresses. They did not need to be more specific than the broad classes of information specified in the 1985 Act, for example, 'national security', 'preventing or detecting serious crime' or 'safeguarding the economic well-being of the United Kingdom'. The combination of a certificate and a warrant formed a 'certified warrant'.
The third stage in the process was filtering. An automated sorting system or search engine, operating under human control, selected communications containing specific search terms or combinations thereof. The search terms would relate to one or more of the certificates issued for the relevant intercepted communications link. Search terms could also be described as 'keyword lists', 'technical databases' or 'The Dictionary'. Search terms and filtering criteria were not specified in certificates, but were selected and administered by State officials without reference to judicial officials or ministers.
Fourth, a system of rules was in place to promote the 'minimisation' of the interference with privacy, namely how to review communications intelligence reports and remove names or material identifying citizens or entities whose details might incidentally have been included in raw material which had otherwise been lawfully intercepted and processed. Where the inclusion of such details in the final report was not proportionate or necessary for the lawful purpose of the warranted interception, it would be removed.
The fifth and final stage in the process was 'dissemination'. Information obtained by an interference with the privacy of communications could be disseminated only where the recipients' purpose(s) in receiving the information was proportionate and necessary in the circumstances. Controls on the dissemination formed a necessary part of Article 8 safeguards.

44. The applicants contended that since the section 3(2) procedure permitted the interception of all communications falling within the large category set out in each warrant, the only protection afforded to those whose communications were intercepted was that the Secretary of State, under section 6(1) of the Act, had to 'make such arrangements as he considers necessary for the purpose of securing that ... so much of the intercepted material as is not certified by the certificate is not read, looked at or listened to by any person' unless the requirements of section 6(2) were met. However, the precise nature of these 'arrangements' were not, at the relevant time, made known to the public, nor was there any procedure available to permit an individual to satisfy him or herself that the 'arrangements' had been followed. The Tribunal did not have jurisdiction to examine such compliance, and although the Commissioner was authorised under section 8 to review the adequacy of the 'arrangements' in general, he had no power to review whether they had been met in an individual case.

45. It was plain that the alleged interception of communications constituted an interference with the applicants' rights under Article 8 § 1. Any such interception, to comply with Article 8 § 2, had to be 'in accordance with the law', and thus have a basis in domestic law that was adequately accessible and formulated with sufficient precision as to be foreseeable. They contended that the United Kingdom legislation breached the requirements of foreseeability. They submitted that it would not compromise national security to describe the arrangements in place for filtering and disseminating intercepted material, and that detailed information about similar systems had been published by a number of other democratic countries, such as the United States of America, Australia, New Zealand, Canada and Germany. The deficiencies in the English system were highlighted by the Court's decision in *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006, which noted that the German legislation set out on its face detailed provisions regulating, *inter alia*, the way in which individual communications were to be selected from the pool of material derived from 'strategic interception'; disclosure of selected material amongst the various agencies of the German State and the use that each could properly make of the material; and the retention or destruction of the material. The authorities' discretion was further regulated and constrained by the public rulings of the Federal Constitutional Court on the compatibility of the provisions with the Constitution. In contrast, in the United Kingdom at the relevant time no provision was made on the face of the statute for any part of the processes following the initial interception, other than the duty on the Secretary of State to make unspecified 'arrangements'. The arrangements themselves were unpublished. There was no legal material in the public domain indicating how the authorities' powers to select, disclose, use or retain particular communications were regulated. The authorities' conduct was not 'in accordance with the law' because it was unsupported by any predictable legal basis satisfying the accessibility principle.

46. In addition, the applicants denied that the interferences pursued a legitimate aim or were proportionate to any such aim, since the 1985 Act permitted interception of large classes of communications for any purpose, and it was only subsequently that this material was sifted to determine whether it fell within the scope of a section 3(2) warrant.

2. The Government

47. For security reasons, the Government adopted a general policy of neither confirming nor denying allegations made in respect of surveillance activities. For the purposes of this application, however, they were content for the Court to proceed on the hypothetical basis that the applicants could rightly claim that communications sent to or from their offices were intercepted at the Capenhurst ETF during the relevant period. Indeed, they submitted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication physically intercepted under a section 3(2) warrant. However, the Government emphatically denied that any interception was being conducted without the necessary warrants and it was their position that, if interception of the applicants' communications did occur, it would have been lawfully sanctioned by an appropriate warrant under section 3(2) of the 1985 Act.

48. The Government annexed to their first set of Observations, dated 28 November 2002, a statement by Mr Stephen Boys Smith, a senior Home Office official, in which it was claimed:

'... Disclosure of the arrangements would reveal important information about the methods of interception used. It is for this reason that the Government is unable to disclose the full detail of the section 6 arrangements for section 3(2) warrants that were in place during the relevant period. The methods to which the relevant documents relate for the relevant period remain a central part of the methods which continue to be used. Therefore, disclosure of the arrangements, the Government assesses and I believe, would be contrary to the interests of national security. It would enable individuals to adapt their conduct so as to minimise the effectiveness of any interception methods which it might be thought necessary to apply to them.

Further, the manuals and instructions setting out the section 6 safeguards and arrangements are in large part not in a form which would be illuminating or readily comprehensible to anyone who had not also undergone the training I have referred to above or had the benefit of detailed explanations. They are couched in technical language and refer to specific techniques and processes which cannot be understood simply from the face of the documents. They contain detailed instructions, precisely in order to ensure that the section 6 arrangements and section 3(2) requirements were fully understood by staff and were fully effective. Any explanations given by the Government of those techniques and processes would compound the problem, referred to above, of undermining the operational effectiveness of the system and techniques used under the authority of warrants.'

The Government stressed, however, that the detailed arrangements were the subject of independent review by the successive Commissioners, who reported that they operated as robust safeguards for individuals' rights (see paragraphs 31-33 above).

49. The Government annexed to their Further Observations, dated 23 May 2003, a second statement by Mr Boys Smith, in response to Mr Campbell's statement (see paragraph 48 above), which provided more detail, to the extent that was possible without undermining national security, about the 'arrangements' made by the Secretary of State under section 6 of the Act. The Government submitted that the Court should proceed on the basis that, in the absence of evidence to the contrary, in the democratic society of the United Kingdom, the relevant ministers, officials and Commissioners properly discharged their statutory duties to ensure that safeguards were in place to comply with all the requirements of section 6. Moreover Mr Boys Smith's statement showed that during the relevant period there was a range of safeguards in place to ensure that the process of selection of material for examination (the stage referred to by the applicants as 'filtering') could be carried out only strictly in accordance with the statutory framework and the terms of the warrant and the certificate (that is, could be carried out only when necessary in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom), and could not be abused or operated arbitrarily.

50. According to Mr Boys Smith, all persons involved in the selection process would have had their attention specifically drawn to the safeguards and limits set out in the primary legislation, which were rigorously applied. Secondly, training was provided to all these persons to emphasise the importance of strict adherence to the operating procedures and safeguards in place. Thirdly, throughout the relevant period operating procedures were in place to ensure that it was not possible for any single individual to select and examine material on an arbitrary and uncontrolled basis. Where, as part of his intelligence gathering, an official wished to intercept and select relevant information, he could not effect the interception himself. He would have to take the request for interception and selection to personnel in a different branch of the department, who would then separately activate the technical processes necessary for the interception and selection to be made. The requesting official would have to set out, in his request, his justification for the selection. Moreover, a record of the request was kept, so that it was possible for others (senior management and the Commissioner) to check back on the official's request, to ensure that it was properly justified. Conversely, it was not possible for the personnel in the branch of the department implementing the technical interception processes to receive the downloaded product of any interception and selection process implemented by them. Therefore, they also could not conduct unauthorised interception and gain access to material themselves. Fourth, there was day-to-day practical supervision of those who conducted the selection processes under section 3(2) warrants ('the requesting officials') by managers

working physically in the same room, who could and would where necessary ask the requesting officials at any time to explain and justify what they were doing. The managers also performed quality control functions in relation to the intelligence reports generated by the requesting officials, and routinely reviewed all intelligence reports incorporating intercepted material that were drawn up by requesting officials for dissemination. Fifth, throughout the relevant period, as was explained to all personnel involved in the selection process, the independent Commissioner had an unrestricted right to review the operation of the selection process and to examine material obtained pursuant to it. From the relevant records, it was possible to check on the interception initiated by officials and, if necessary, to call for an explanation. Each of the Commissioners during the relevant period (Lords Lloyd, Bingham and Nolan) exercised his right to review the operation of the selection processes, and each Commissioner declared himself satisfied that the selection processes were being conducted in a manner that was fully consistent with the provisions of the 1985 Act. By this combination of measures there were effective safeguards in place against any risk of individual, combined or institutional misbehaviour or action contrary to the terms of the legislation or warrant. Finally, once the Intelligence Services Act 1994 had come into force on 15 December 1994, it was possible for an aggrieved individual to complain to the Tribunal.

51. As regards the processes described by the applicants as 'minimisation' and 'dissemination', safeguards in place during the relevant period ensured that access to and retention of the raw intercept material and any intelligence reports based on such material were kept to the absolute minimum practicable, having regard to the public interest served by the interception system. Relevant information in the material selected and examined was disseminated in the form of intelligence reports, usually compiled by the requesting officials. As part of the safeguards under section 6 of the 1985 Act, there were throughout the relevant period internal regulations governing the manner in which intelligence reports were produced, directed at all individuals engaged in producing intelligence reports based on material selected from communications intercepted under the section 3(2) warrant regime. The regulations stipulated, among other things, that no information should be reported unless it clearly contributed to a stated intelligence requirement conforming to one of the purposes set out in section 2(2) of the 1985 Act. The regulations also dealt specifically with the circumstances in which it was appropriate to name specific individuals or organisations in the intelligence reports. During the relevant period there was in place a comprehensive security regime for handling all types of classified material. Dissemination was restricted to those with a genuine 'need to know', and was further limited to persons who had been security vetted and briefed on how to handle it, with a view to ensuring continued confidentiality.

52. The Government refuted the suggestion that, to comply with Article 8 § 2, the safeguards put in place in respect of the intercepted material had themselves to comply with the 'in accordance with the law' criteria. In any event, the functions of the Commissioner and the Tribunal were embodied in statutory provisions that were sufficiently certain and accessible, and in assessing whether the 'foreseeability' requirements of Article 8 § 2 had been met, it was legitimate to take into account the existence of general safeguards against abuse such as these (the Government relied on *Association for European Integration and Human Rights and Ekimzhiev v. Bulgaria*, no. 62540/00, §§ 77-94, 28 June 2007 and *Christie v. the United Kingdom*, no. 21482/93, Commission decision of 27 June 1994). Moreover, the 1985 Act provided that interception was criminal except where the Secretary of State had issued a warrant and sections 2 and 3(2) set out in very clear terms that, during the relevant period, any person in the United Kingdom who sent or received any form of telecommunication outside Britain could in principle have had it intercepted pursuant to such a warrant. The provisions of primary legislation were, therefore, sufficient to provide reasonable notice to individuals to the degree required in this particular context, and provided adequate protection against arbitrary interference. Article 8 § 2 did not require that the nature of the 'arrangements' made by the Secretary of State under section 6 of the 1985 Act be set out in legislation (see *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, § 68), and for security reasons it had not been possible to reveal such information to the public, but the arrangements had been subject to review by the Commissioners, each of whom had found them to be satisfactory (see paragraph 33 above).

53. The Government submitted that the section 3(2) warrant regime was proportionate and 'necessary in a democratic society'. Democratic States faced a growing threat from terrorism, and as communications networks became more wide-ranging and sophisticated, terrorist organisations had acquired ever greater scope to operate and co-operate on a trans-national level. It would be a gross dereliction of the Government's duty to safeguard national security and the lives and well-being of its population if it failed to take steps to gather intelligence that might allow preventative action to be taken or if it compromised the operational effectiveness of the surveillance methods available to it. Within the United Kingdom the Government had extensive powers and resources to investigate individuals and organisations that might threaten the interests of national security or perpetrate serious crimes, and it was therefore feasible for the domestic interception regime to require individual addresses to be identified before interception could take place. Outside the jurisdiction, however, the ability of the Government to discover the identity and location of individuals and organisations which might represent a threat to national security was drastically reduced and a broader approach was needed. Maintaining operational effectiveness required not simply that the fact of interception be kept as secret as appropriate; it was also necessary to maintain a degree of secrecy as regards the methods by which such interception might be effected, to prevent the loss of important sources of information.
54. The United Kingdom was not the only signatory to the Convention to make use of a surveillance regime involving the interception of volumes of communications data and the subsequent operation of a process of selection to obtain material for further consideration by government agencies. It was difficult to compare the law and practice of other democratic States (such as the German system of strategic monitoring examined by the Court in the *Weber and Saravia* case cited above), since each country had in place a different set of safeguards. For example, the United Kingdom did not permit intercepted material to be used in court proceedings, whereas many other States did allow this, and there were few, if any, direct equivalents to the independent Commissioner system created by the 1985 Act. Moreover, it was possible that the operational reach of the United Kingdom's system had had to be more extensive, given the high level of terrorist threat directed at the United Kingdom during the period in question.

A. Admissibility
55. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits
1. Whether there was an interference
56. Telephone, facsimile and e-mail communications are covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8 (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 77, 29 June 2006, and the cases cited therein). The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (see *Weber and Saravia*, cited above, § 78).
57. The Court notes that the Government are prepared to proceed, for the purposes of the present application, on the basis that the applicants can claim to be victims of an interference with their communications sent to or from their offices in the United Kingdom and Ireland. In any event, under section 3(2) the 1985 Act, the authorities were authorised to capture communications contained within the scope of a warrant issued by the Secretary of State and to listen to and examine communications falling within the terms of a certificate, also issued by the Secretary of State (see paragraphs 23-24 above). Under section 6 of the 1985 Act arrangements had to be made regulating the disclosure, copying and storage of intercepted material (see paragraph 27 above). The Court considers that the existence of these powers,

particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied (see *Weber and Saravia*, cited above, §§ 78-79).

2. Whether the interference was justified

58. Such an interference is justified by the terms of paragraph 2 of Article 8 only if it is 'in accordance with the law', pursues one or more of the legitimate aims referred to in paragraph 2 and is 'necessary in a democratic society' in order to achieve the aim or aims (see *Weber and Saravia*, cited above, § 80).

3. Whether the interference was 'in accordance with the law'

a. General principles

59. The expression 'in accordance with the law' under Article 8 § 2 requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him (see, among other authorities, *Kruslin v. France*, judgment of 24 April 1990, Series A no. 176-A, § 27; *Huvig v. France*, judgment of 24 April 1990, Series A no. 176-B, § 26; *Lambert v. France*, judgment of 24 August 1998, *Reports of Judgments and Decisions* 1998-V, § 23; *Perry v. the United Kingdom*, no. 63737/00, § 45, ECHR 2003-IX; *Dumitru Popescu v. Romania (No. 2)*, no. 71525/01, § 61, 26 April 2007).

60. It is not in dispute that the interference in question had a legal basis in sections 1-10 of the 1985 Act (see paragraphs 16-27 above). The applicants, however, contended that this law was not sufficiently detailed and precise to meet the 'foreseeability' requirement of Article 8(2), given in particular that the nature of the 'arrangements' made under section 6(1)(b) was not accessible to the public. The Government responded, relying on paragraph 68 of *Malone* (cited above), that although the scope of the executive's discretion to carry out surveillance had to be indicated in legislation, 'the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law'.

61. The Court observes, first, that the above passage from *Malone* was itself a reference to *Silver and Others*, also cited above, §§ 88-89. There the Court accepted that administrative Orders and Instructions, which set out the detail of the scheme for screening prisoners' letters but did not have the force of law, could be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the relevant primary and secondary legislation, but only to 'the admittedly limited extent to which those concerned were made sufficiently aware of their contents'. It was only on this basis – that the content of the Orders and Instructions were made known to the prisoners – that the Court was able to reject the applicants' contention that the conditions and procedures governing interferences with correspondence, and in particular the directives set out in the Orders and Instructions, should be contained in the substantive law itself.

62. More recently, in its admissibility decision in *Weber and Saravia*, cited above, §§ 93-95, the Court summarised its case-law on the requirement of legal 'foreseeability' in this field as follows (and see also *Association for European Integration and Human Rights and Ekimzhiev*, cited above, §§ 75-77):

'93. ... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, *inter alia*, *Leander* [*v. Sweden*, judgment of 26 August 1987, Series A no. 116], p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, *inter alia*, *Malone*, cited above, p. 32, § 67; *Huvig*, cited above, pp. 54-55, § 29; and *Rotaru* [*v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V]). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, *Reports* 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, cited above, p. 541, § 64; *Huvig*, cited above, pp. 54-55, § 29; and *Valenzuela Contreras*, ibid.).

94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, pp. 32-33, § 68; *Leander*, cited above, p. 23, § 51; and *Huvig*, cited above, pp. 54-55, § 29).

95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003).'

63. It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses (the equivalent, within the United Kingdom, of the section 3(1) regime). However, the *Weber and Saravia* case was itself concerned with generalised 'strategic monitoring', rather than the monitoring of individuals (cited above, § 18). The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other. The Court's approach to the foreseeability requirement in this field has, therefore, evolved since the Commission considered the United Kingdom's surveillance scheme in its above-cited decision in *Christie v. the United Kingdom*.

b. Application of the general principles to the present case

64. The Court recalls that section 3(2) of the 1985 Act allowed the executive an extremely broad discretion in respect of the interception of communications passing between the United Kingdom and an external receiver, namely to intercept 'such external communications as are described in the warrant'. There was no limit to the type of external communications which could be included in a section 3(2) warrant. According to the applicants, warrants covered very broad classes of communications, for example, 'all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe', and all communications falling within the specified category would be physically intercepted (see paragraph 43 above). In their observations to the Court, the Government accepted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication intercepted under a section 3(2) warrant (see paragraph 47 above). The legal discretion granted to the executive for the physical capture of external communications was, therefore, virtually unfettered.

65. Moreover, the 1985 Act also conferred a wide discretion on the State authorities as regards which communications, out of the total volume of those physically captured, were listened to or read. At the time of issuing a section 3(2) interception warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. Again, according to the applicants, certificates were formulated in general terms and related only to intelligence tasks and priorities, such as, for example, 'national security', 'preventing or detecting serious crime' or 'safeguarding the economic well-being of the United Kingdom' (see paragraph 43 above). On the face of the 1985 Act, only external communications emanating from a particular address in the United Kingdom could not be included in a certificate for examination unless the Secretary of State considered it necessary for the prevention or detection of acts of terrorism (see paragraphs 23-24 above). Otherwise, the legislation provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy.

66. Under section 6 of the 1985 Act, the Secretary of State, when issuing a warrant for the interception of external communications, was called upon to 'make such arrangements as he consider[ed] necessary' to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary. The applicants contend that material was selected for examination by an electronic search engine, and that search terms, falling within the broad categories covered by the certificates, were selected and operated by officials (see paragraph 43 above). According to the Government (see paragraphs 48-51 above), there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that details of these 'arrangements' made under section 6 were not contained in legislation or otherwise made available to the public.

67. The fact that the Commissioner in his annual reports concluded that the Secretary of State's 'arrangements' had been complied with (see paragraphs 32-33 above), while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the 'arrangements' were. In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, *inter alia*, should be set out in a form which is open to public scrutiny and knowledge.

68. The Court notes the Government's concern that the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk. However, it observes that the German authorities considered it safe to include in the G10 Act, as examined in *Weber and Saravia* (cited above), express provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order (op. cit., § 32). Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act (see *Weber and Saravia*, cited above, § 100). The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications (op. cit., §§ 33-50). In the United Kingdom, extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain (see paragraph 40 above), which suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.

69. In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, 'in accordance with the law'.

70. It follows that there has been a violation of Article 8 in this case.

(...)

FOR THESE REASONS, THE COURT UNANIMOUSLY
1. *Declares* the application admissible;
2. *Holds* that there has been a violation of Article 8 of the Convention (..);

(...)'

NOOT

1. Deze uitspraak is van belang, omdat het Hof hierin een nadere invulling geeft aan de eis van voorzienbaarheid bij wet, voortvloeiend uit art. 8 EVRM, bij het onderscheppen en monitoren van telefoon-, e-mail en dataverkeer. In zijn uitspraak *Weber-Saravia t. Duitsland* (EHRM 29 juni 2006, nr. 54934/00, *EHRC* 2007, 13 (m.nt. JPL)) oordeelde het Hof dat Duitse wetgeving betreffende het monitoren van telecommunicatie voldoende waarborgen omvatte om misbruik en te ruim gebruik van de gecreëerde afluisterbevoegdheden te voorkomen en een adequate onafhankelijke rechtmatigheidscontrole over de uitoefening van die bevoegdheden te garanderen. In de onderhavige uitspraak brengt het Hof enkele verfijningen aan op zijn in *Weber en Saravia* geformuleerde maatstaven en oordeelt het dat de Britse wetgeving inzake de afluisterbevoegdheden – in tegenstelling tot de Duitse – niet aan deze maatstaven voldoet. Ook geeft het Hof een nadere uitleg over de ratio van deze maatstaven. In het onderstaande worden deze twee aspecten belicht.

2. In zowel *Weber en Saravia* als de onderhavige zaak stond het zogeheten *strategic monitoring* centraal: het met behulp van satellietschotels en andere ICT-toepassingen systematisch onderscheppen en monitoren van in beginsel alle telecommunicatieverkeer, in het bijzonder telefoon- en e-mailverkeer, in een bepaald gebied of via bepaalde communicatiekanalen (bijvoorbeeld satellieten of kabels). Daarbij wordt met bepaalde zoektermen door een opsporings- of veiligheidsdienst gefilterd op berichten die betrekking hebben op bepaalde ernstige misdrijven of bedreigingen van de nationale veiligheid, in het bijzonder terroristische aanslagen. Reeds in 2001 ontstond in meerdere Europese landen, waaronder het Verenigd Koninkrijk en Nederland, ophef over *Echelon*, een geheim satellietsysteem waarmee door de Verenigde Staten, het Verenigd Koninkrijk en enkele andere staten alle ter wereld gevoerde telecommunicatieverkeer zou kunnen worden afgeluisterd.[1] De Nederlandse minister van Defensie schreef in antwoord op Kamervragen dat het bestaan van *Echelon* aannemelijk was, maar dat er ook andere systemen waren die de aan 'Echelon' toegeschreven mogelijkheden bezitten.[2] Over de precieze capaciteit en locaties van de betreffende systemen is tot op heden weinig bekend.[3] Uit de onderhavige

1 Zie ook over Echelon: J.P. Loof in zijn noot bij EHRM 29 juni 2006, nr. 54934/00, *EHRC* 2007, 13, p. 128 e.v.
2 *Kamerstukken II* 2000/01, 27 591, nr. 1.
3 Zie over grootschalig afluisteren in de Nederlandse context: Verslag van het Algemeen Overleg over grootschalig afluisteren van telecommunicatiesystemen van 29 januari 2002, *Kamerstukken II* 2001/02, 27 591, nr. 3; Notitie *Grootschalig afluisteren van moderne telecommunicatiesystemen* en aanbiedingsbrief van de minister van Binnenlandse Zaken en Koninkrijksrelaties van 4 april 2002, *Kamerstukken II* 2001/02, 27 591, nr. 4 en bijlage; Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst, *De AIVD in verandering*, bijlage bij *Kamerstukken II* 2004/05, 29 876, nr. 1; alsmede het Jaarverslag van de AIVD 2007 (p. 99-101), over de Nationale Sigint

uitspraak van het EHRM, in samenhang gelezen met de uitspraak inzake Weber en Saravia van 2006, blijkt wel dat de voornoemde opmerking van de minister van Defensie over het bestaan van meerdere systemen juist was.

3. Ten aanzien van de vraag of in de onderhavige zaak jegens de klagers – de mensenrechtenorganisaties *Liberty, British Irish Rights Watch* en de *Irish Council for Civil Liberties* – sprake was van een inbreuk op het door art. 8 EVRM beschermde recht op respect voor het privé-leven overweegt het Hof, onder verwijzing naar *Weber en Saravia* (§ 77-79), dat het enkele bestaan van wetgeving betreffende een systeem voor het heimelijk monitoren van communicatie een dreiging om te worden afgeluisterd met zich brengt voor een ieder op wie deze wetgeving van toepassing kan zijn. Deze dreiging raakt noodzakelijkerwijs aan de communicatievrijheid van de gebruikers van telecommunicatiediensten en vormt reeds om die reden een inbreuk op het recht op respect voor het privé-leven van de klagers, onafhankelijk van de vraag welke daadwerkelijke maatregelen jegens hen zijn genomen. Op grond van artikel 3, tweede lid, van de Britse Wet op de Onderschepping van Communicatie 1985 waren de Britse autoriteiten bevoegd om op grond van een machtiging, gegeven door de Britse Minister van Binnenlandse Zaken, communicatie te onderscheppen, beluisteren en doorzoeken, voor zover deze handelingen voldeden aan de eisen opgenomen in een door deze minister afgegeven certificaat (de zogeheten 'gecertificeerde machtiging'). Ingevolge artikel 6 van deze wet diende lagere regelgeving te worden vastgesteld betreffende het doorzoeken, kopiëren en bewaren van het onderschepte materiaal. Het Hof overweegt dat het bestaan van deze bevoegdheden, in het bijzonder die betreffende het onderzoeken, het gebruik en het opslaan van de onderschepte communicatiegegevens, een inbreuk oplevert van de rechten van klagers onder art. 8 EVRM, aangezien zij (rechts)personen zijn jegens wie deze bevoegdheden konden worden toegepast. Met deze bewoordingen legt het Hof het accent op het feit dat *strategic monitoring* élke burger raakt die zich in het betrokken land bevindt: niet alleen degenen jegens wie door de minister aan de veiligheidsdiensten een machtiging is afgegeven om 'op naam' te zoeken, gesprekken af te luisteren en e-mails te openen, doch een ieder wiens telefoongesprekken en e-mails via de betrokken kanalen wordt getransporteerd. In dit kader kan voorts worden gewezen op een procesrechtelijk aspect van deze uitspraak, namelijk het feit dat de klagers niet-gouvernementele organisaties (NGOs) zijn en geen natuurlijke personen. Op grond van artikel 34 EVRM kan een klacht worden ingediend door iedere natuurlijke persoon, iedere niet-gouvernementele organisatie en iedere groep personen, onder de voorwaarde dat de identiteit van de leden van de groep bekend is en ieder lid van de groep beweert slachtoffer te zijn van een verdragsschen-

Organisatie, een samenwerkingsverband tussen de AIVD en de MIVD inzake de onderschepping van niet-kabelgebonden telecommunicatie, bijlage bij *Kamerstukken II* 2007/08, 30 977, nr. 9. In dit verband zij voorts gewezen op art. 27 van de Wet op de inlichtingen- en veiligheidsdiensten (bevoegdheid tot het met een technisch hulpmiddel ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie) en op het voorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten in verband met de verbetering van de mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede enkele andere wijzigingen (*Kamerstukken I* 2007/08, 30 553, nr. A), in het bijzonder het daarin voorgestelde art. 12a (bevoegdheid voor de diensten tot het uitvoeren van geautomatiseerde data-analyse), alsmede op het advies van het College bescherming persoonsgegevens over dit wetsvoorstel van 20 december 2007, gepubliceerd op www.cbpweb.nl.

ding.[4] Onder het procesrecht van het EVRM is het voor rechtspersonen niet mogelijk op te komen voor een collectieve actie. In de onderhavige zaak hadden de drie NGOs echter gesteld dat zij zelf slachtoffer waren van een schending van artikel 8 EVRM (omdat hun communicatie werd gemonitord) en verklaarde het Hof hen ontvankelijk in hun klacht.

4. Het kernpunt in de onderhavige uitspraak betrof de eis van voorzienbaarheid bij wet. Het Hof stelt, onder verwijzing naar *Silver and Others t. Verenigd Koninkrijk*,[5] voorop dat lagere, administratieve regels in aanmerking kunnen worden genomen bij het onderzoek naar de vraag of is voldaan aan de eis van voorzienbaarheid, maar slechts voor zover degenen die door deze regels worden geraakt zich in voldoende mate bewust zijn van de inhoud van deze regels. Vervolgens overweegt het Hof dat het, in de context van het onderscheppen en afluisteren van communicatie, essentieel is dat er duidelijke en gedetailleerde regelgeving is, vooral omdat de beschikbare technologie voor het gebruik van het onderschepte berichtenverkeer steeds geavanceerder wordt. Aldus wordt aan burgers duidelijk onder welke omstandigheden en voorwaarden de autoriteiten zijn gemachtigd om zulke bevoegdheden jegens hen te gebruiken. In eerdere jurisprudentie, onder meer in *Malone t. het Verenigd Koninkrijk*,[6] *Leander t. Sweden*,[7] *Huvig t. Frankrijk*,[8] *Valenzuela Contreras t. Spanje*,[9] *Kopp. t. Zwitserland*,[10] en *Rotaru t. Roemenië*[11] heeft het Hof een aantal beginselen en eisen geformuleerd voor het heimelijk onderscheppen en afluisteren van communicatie, teneinde misbruik te voorkomen. Dit betreft onder meer eisen voor de duur van het afluisteren en procedures voor het gebruik en de opslag van de data.[12] Het Hof overweegt dat deze beginselen en eisen oorspronkelijk zijn ontwikkeld in het kader van afluisterpraktijken ten aanzien van specifieke personen, maar er geen reden is om deze niet ook toe te passen bij meer algemene afluisterprogramma's. In de onderhavige Britse zaak waren er weliswaar interne regels vastgesteld voor het doorzoeken, het gebruik en de opslag van de onderschepte communicatiegegevens, maar deze regels waren niet vastgelegd in wetgeving op of andere wijze toegankelijk gemaakt voor het publiek. Het Hof concludeert dat het Britse rechtssysteem niet in voldoende duidelijke mate de reikwijdte en randvoorwaarden voor de afluisterbevoegdheden formuleert en dat de inbreuk op de rechten van de klagers onder artikel 8 EVRM derhalve niet voldeed aan de eis van voorzienbaarheid bij wet.

4 Zie uitgebreid over de bevoegdheid *ratione personae*: T. Barkhuysen en M.L. van Emmerik, *Procederen over mensenrechten onder het EVRM, het IVBPR en andere VN-verdragen*, Nijmegen: Ars Aequi Libri 2008, p. 42 e.v.
5 EHRM 25 maart 1983, no. 5947/72.
6 EHRM 2 augustus 1984, no. 8691/79, *NJ* 1988, 534 (m. nt. PVD).
7 EHRM 26 maart 1987, no. 9248/81, *NJCM-Bulletin* 1988, p. 148-166 (m. nt. ThLB).
8 EHRM 24 april 1990, no. 11105/84, *NJCM-Bulletin* 1990, p. 704-714 (m. nt. EM).
9 EHRM, 30 juli 1998, no. 27671/95, NJB 1998, 35, p. 1603.
10 EHRM 25 maart 1998, no. 13/1997/797/1000, *NJCM-Bulletin* 1998, p. 860-883 (m. nt. EM).
11 EHRM 4 mei 2000, no. 28341/95, EHRC 2000, 53 (m. nt. EB).
12 Zie voor een analyse van deze jurisprudentie: A.W. Heringa en L. Zwaak, 'Chapter 12 – right to respect for privacy (Article 8)', in: P. van Dijk, F. van Hoof, A. van Rijn en L. Zwaak (red.), *Theory and Practice of the European Convention on Human Rights*, Antwerpen-Oxford: Intersentia 2006, p. 666-674 en 734-738; P. de Hert, 'Artikel 8 – Recht op privacy', in: J. Vande Lanotte en Y. Haeck (eds.), *Handboek EVRM*, Deel 2 Artikelsgewijs Commentaar, Volume I, p. 769-771 en 777-780.