Annotation: EHRM 2007-10-16

Groothuis, M.M.

to reveal his identity from the beginning of the proceedings. In this case, however, as stated above, the Commission has not shown that, at the time they participated in the meeting in question, the persons concerned had reasonable grounds for believing that they enjoyed confidential treatment of any kind, or that they had asked the Commission not to reveal their identity. Moreover, as stated in paragraph 137 above, given that the Commission disclosed the minutes, albeit with certain names removed, it must have taken the view that this was not information covered by business secrecy. Finally, the Commission has not put forward any argument to demonstrate in what way disclosure of the names of the persons who refused their consent could have harmed any investigations involved in this case.
155. In those circumstances, the arguments based on protection of the purposes of inspections and investigations cannot succeed.
156. There is therefore no need to examine the possible existence of a higher public interest justifying disclosure of the document concerned.
157. It follows from the whole of the above that the full minutes of the meeting of 11 October 1996, containing all the names, does not fall within the exceptions under Article 4(1)(b) or the third indent of Article 4(2) of Regulation No 1049/2001.
158. The contested decision must therefore be annulled.

Costs
159. Under Article 87(2) of the Rules of Procedure, the unsuccessful party is to be ordered to pay the costs if they have been applied for in the successful party's pleadings. Since the Commission has been unsuccessful, it must be ordered to pay the applicant's costs, as the applicant has pleaded.
160. Under the third subparagraph of Article 87(4) of the Rules of Procedure, the Court of First Instance may order an intervener to bear his own costs. In this case, the intervener in support of the applicant is ordered to bear his own costs.

On those grounds, the Court of First Instance (Third Chamber)
hereby:
1. Annuls the Commission's decision of 18 March 2004, rejecting an application for access to the full minutes of the meeting of 11 October 1996, containing all the names;
2. Orders the Commission to pay the costs incurred by The Bavarian Lager Co. Ltd;
3. Orders the European Data Protection Supervisor (EDPS) to bear his own costs.

3

Europees Hof voor de Rechten van de Mens
16 oktober 2007, nr. 74336/01
(Bratza (President), Cadadevall, Bonello, Steiner, Pavlovschi, Garlicki, Mijović)
Noot Groothuis

Recht op respect voor privéleven. Doorzoeken van digitale bestanden op advocatenkantoor. Niet-inachtneming van naar nationaal recht geldende procedurele waarborgen.

[EVRM art. 8, 41]

Wieser is advocaat te Salzburg en eigenaar en manager van Bicos Beteiligungen GmbH (verder: Bicos), een holding company die onder meer eigenaar is van de BV Novamed. Bicos en Novamed zijn gevestigd in het advocatenkantoor van Wieser. In het kader van een strafrechtelijk onderzoek naar illegale handel in medicijnen is in 2000 een aantal aan Novamed geadresseerde facturen gevonden. Op verzoek van het OM gaf de Rechtbank Salzburg het bevel strafrechtelijk onderzoek te verrichten in de kantoren van Bicos en Novamed en daarbij alle documenten te verzamelen die duidden op contacten met de verdachte personen en bedrijven.
In oktober 2000 werd het kantoor van Bicos, tevens het advocatenkantoor van Wieser, doorzocht. Eén team politiefunctionarissen doorzocht het kantoor in aanwezigheid van Wieser zelf en een vertegenwoordiger van de Orde van Advocaten. Daarbij werd een door Oostenrijks recht voorgeschreven procedure gevolgd (art. 152 Wetboek van Strafvordering), waarbij elk document, alvorens te worden ingenomen, werd getoond aan Wieser en de vertegenwoordiger van de Orde. Wanneer Wieser bezwaar maakte, werd het betreffende document verzegeld en gedeponeerd bij de rechtbank. Ook werd een lijst gemaakt van de ingenomen documenten en werd een onderzoeksverslag opgesteld en on-

dertekend. Een tweede team politiefunctionarissen voerde gelijktijdig een onderzoek uit naar de computerapparatuur van Wieser. De vertegenwoordiger van de Orde werd hierover geïnformeerd en was gedurende een deel van dit onderzoek aanwezig. Na afloop vertrok dit politieteam zonder een onderzoeksverslag te hebben opgesteld en zonder Wieser te hebben geïnformeerd over de resultaten. Later die dag werd alsnog een verslag van het digitale onderzoek opgesteld. Het vermeldde dat was gezocht naar bestanden met de namen van de verdachte personen en bedrijven en dat 91 bestanden die deze namen bevatten, waren gekopieerd naar computerschijven van de politie.

Wieser klaagde bij de rechtbank te Salzburg over schending van zijn beroepsgeheim als advocaat en over schending van art. 152 Wetboek van Strafvordering. De rechtbank verwierp zijn beroep. Ook Wiesers hoger beroep bij het College van Administratief Beroep van Salzburg werd verworpen.

Het EHRM stelt voorop dat het doorzoeken en in beslag nemen van elektronische data in een advocatenkantoor een inbreuk vormt op art. 8 EVRM. Het Hof stelt vast dat strafrechtelijk onderzoek een legitiem doel diende: het voorkomen van strafbare feiten. Ten aanzien van de proportionaliteit van de inbreuk onderzoekt het Hof of het nationale recht voldoende en effectieve waarborgen biedt tegen misbruik en willekeur. In casu was het onderzoek uitgevoerd op bevel van een onderzoeksrechter in het kader van een strafrechtelijk onderzoek naar illegale handel in medicijnen, gebaseerd op het feit dat facturen met de naam Novamed waren gevonden. Het Hof oordeelt dat het onderzoek op het kantoor van Wieser derhalve gebaseerd was op een redelijke verdenking. Vervolgens overweegt het Hof dat het Oostenrijkse recht een aantal waarborgen bevat met betrekking tot het in beslag nemen van documenten en elektronische bestanden. Het Hof stelt vast dat deze eisen en regels in acht zijn genomen ten aanzien van de papieren documenten, maar niet ten aanzien van de elektronische data. Schending art. 8 EVRM t.a.v. Wieser.

De wijze waarop het onderzoek is uitgevoerd bracht naar het oordeel van het Hof ook het risico met zich dat het beroepsgeheim van Wieser als advocaat zou worden geschonden. Weliswaar was Wieser niet de advocaat van Bicos of Novamed, maar hij heeft aangegeven wel advocaat te zijn van een aantal bedrijven waarvan Bicos aandeelhouder was. Schending van art. 8 EVRM t.a.v. Bicos.

Wieser en Bicos Beteiligungen GmbH
tegen
Oostenrijk

The Law

I. Alleged violation of Article 8 of the Convention

41. The applicants complain about the search and seizure of electronic data. They rely on Article 8 of the Convention which reads as follows:

"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. Applicability of Article 8

42. The Government based their comments on the assumption that the search and seizure at issue interfered with the applicants' "private life" and "home".

43. The Court reiterates that the search of a lawyer's office has been regarded as interfering with "private life" and "correspondence" and, potentially, home, in the wider sense implied by the French text which uses the term "*domicile*" (see *Niemietz v. Germany*, judgment of 16 December 1992, Series A no. 251-B, pp. 33–35, §§ 29–33, and *Tamosius v. the United Kingdom* (dec.), no. 62002/00, ECHR 2002-VIII; see also *Petri Sallinen and Others v. Finnland*, no. 50882/99, § 71, 27 September 2005, which confirms that the search of a lawyer's business premises also interfered with his right to respect for his "home"). The search of a company's business premises was also found to interfere with its right to respect for its "home" (see *Société Colas Est and Others v. France*, no. 37971/97, ECHR 2002-III, §§ 40–42).

44. In the present case, the applicants do not complain about the search of their business premises, which are the first applicant's law office and the applicant company's seat nor do they complain about the seizure of documents.

They only complain in respect of the search and seizure of electronic data.

45. The Court considers that the search and seizure of electronic data constituted an interference with the applicants' right to respect for their "correspondence" within the meaning of Article 8 (see *Niemietz*, cited above, pp. 34–35, § 32 as regards a lawyer's business correspondence, and *Petri Sallinen and Others*, cited above, § 71, relating to the seizure of a lawyer's computer disks). Having regard to its above-cited case-law extending the notion of "home" to a company's business premises, the Court sees no reason to distinguish between the first applicant, who is a natural person, and the second applicant, which is a legal person, as regards the notion of "correspondence". It does not consider it necessary to examine whether there was also an interference with the applicants' "private life".

46. The Court must therefore determine whether the interference with the applicants' right to respect for their correspondence satisfied the requirements of paragraph 2 of Article 8.

B. Compliance with Article 8

1. The parties' submissions

47. The Court observes at the outset that in its admissibility decision of 16 May 2006 it joined the Government's objection as to non-exhaustion to the merits. The Government argued that the applicants had failed to make use of the possibility, provided for in the Code of Criminal Procedure, to request that documents or data be sealed and deposited with the court in order to obtain a court decision on whether or not they may be used for the investigation. The applicants contested this view, arguing that the manner in which the search was carried out had deprived them of the possibility to make effective use of their rights.

48. On the merits, the applicants asserted that the search and seizure of electronic data had been disproportionate. They claimed that the first applicant was not only the manager of the applicant company but also its counsel and the counsel of Novamed. Thus the search had necessarily led to correspondence, for instance letters and file notes that the first applicant had made in his capacity as counsel. During the search of the paper documents all such documents had either been removed immediately or sealed and returned to the applicant by the investigating judge as being subject to professional secrecy. In contrast, the electronic data had been seized without observing the attendant procedural guarantees. In this connection the applicants relied on the same arguments as submitted in respect of the issue of exhaustion of domestic remedies.

49. The applicants maintained that the applicant company's rights had also been infringed, since it had had no control over the kind of data that were seized. The search for the word Bicos had necessarily led to data unrelated to the subject defined in the search warrant. The procedural guarantees laid down in the Code of Criminal Procedure had not been complied with, since the applicant company had not been given the possibility to have the data sealed and to obtain a decision by the investigating judge as to which data might be used for the investigation.

50. The Government noted at the outset that the applicants only complained about the search of electronic data and that their submissions essentially related to the first applicant's position as a lawyer and to the alleged lack of safeguards to protect his duty of professional secrecy, while the complaint as regards the applicant company remained unsubstantiated.

51. Referring to the Court's case-law, the Government argued that the search and seizure of electronic data had a legal basis in the Code of Criminal Procedure and served legitimate aims, namely the prevention of crime and the protection of health.

52. As regards the necessity of the interference, the Government asserted that the search and seizure of the data had been proportionate to the legitimate aim pursued. The contested measures had been ordered by a judicial search warrant which had delimited their scope. Moreover, Austrian law contained specific procedural safeguards for the search of a lawyer's office. They had been complied with in that the search had taken place in the presence of the applicant and a representative of the Bar Association, whose role had been to ensure that the search did not encroach on the first applicant's duty of professional secrecy. In accordance with the search warrant, the first applicant's computer facilities had been searched with the help of certain key words, that is, the names of

the firms involved, Novamed and Bicos, and the names of the suspects in the proceedings conducted in Italy. Since the first applicant was not the second applicant's counsel, their lawyer-client relationship had not been affected. Moreover, the representative of the Bar Association had been informed of the search of the first applicant's computer facilities and the search procedure documented in the data securing report. The fact that the said report had not been drawn up during the search but later the same day was not decisive, since the main aim of recording which data had been seized had been achieved.

2. The Court's assessment

(a) In accordance with the law

53. The Court reiterates that an interference cannot be regarded as "in accordance with the law" unless, first of all, it has some basis in domestic law. In relation to Article 8 § 2 of the Convention, the term "law" is to be understood in its "substantive" sense, not in its "formal" one. In a sphere covered by the written law, the "law" is the enactment in force as the competent courts have interpreted it (see *Société Colas Est and Others*, cited above, § 43, with further references, and *Petri Sallinen and Others*, cited above, § 77).

54. The Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data (see paragraph 34 above). In fact, the applicants do not contest that the measures complained of had a basis in domestic law.

(b) Legitimate aim

55. The Court observes that the search and seizure was ordered in the context of criminal proceedings against third persons suspected of illegal trade in medicaments. It therefore served a legitimate aim, namely, the prevention of crime.

(c) Necessary in a democratic society

56. The parties' submissions concentrated on the necessity of the interference and in particular on the question whether the measures were proportionate to the legitimate aim pursued and whether the procedural safeguards provided for by the Code of Criminal Procedure were adequately complied with.

57. In comparable cases, the Court has examined whether domestic law and practice afforded adequate and effective safeguards against any abuse and arbitrariness (see, for instance, *Société Colas Est and Others*, cited above, § 48). Elements taken into consideration are, in particular, whether the search was based on a warrant issued by a judge and based on reasonable suspicion, whether the scope of the warrant was reasonably limited and – where the search of a lawyer's office was concerned – whether the search was carried out in the presence of an independent observer in order to ensure that materials subject to professional secrecy were not removed (see *Niemietz*, cited above, p. 36, § 37, and *Tamosius*, cited above).

58. In the present case, the search of the applicants' computer facilities was based on a warrant issued by the investigating judge in the context of legal assistance for the Italian authorities which were conducting criminal proceedings for illegal trade in medicaments against a number of companies and individuals. It relied on the fact that invoices addressed to Novamed, 100% owned by the applicant company, had been found. In these circumstances, the Court is satisfied that the search warrant was based on reasonable suspicion.

59. The Court also finds that the search warrant limited the documents or data to be looked for in a reasonable manner, by describing them as any business documents revealing contacts with the suspects in the Italian proceedings. The search remained within these limits, since the officers searched for documents or data containing either the word Novamed or Bicos or the name of any of the suspects.

60. Moreover, the Code of Criminal Procedure provides further procedural safeguards as regards the seizure of documents and electronic data. The Court notes the following provisions of the Code:

(a) The occupant of premises searched shall be present;

(b) A report is to be drawn up at the end of the search and items seized are to be listed;

(c) If the owner objects to the seizure of documents or data carriers they are to be sealed and put before the judge for a decision as to wheth-

er or not they are to be used for the investigation; and
(d) In addition, as far as the search of a lawyer's office is concerned, the presence of a representative of the Bar Association is required.
61. The applicants' claim is not that the guarantees provided by Austrian law are insufficient but that they were not complied with in the present case as regards the seizure of data. The Court notes that a number of officers carried out the search of the applicants' premises. While one group proceeded to the seizure of documents, the second group searched the computer system using certain search criteria and seized data by copying numerous files to disks.
62. The Court observes that the safeguards described above were fully complied with as regards the seizure of documents: whenever the representative of the Bar Association objected to the seizure of a particular document, it was sealed. A few days later the investigating judge decided in the presence of the applicant which files were subject to professional secrecy and returned a number of them to the applicant on this ground. In fact, the applicants do not complain in this respect.
63. What is striking in the present case is that the same safeguards were not observed as regards the electronic data. A number of factors show that the exercise of the applicants' rights in this respect was restricted. First, the member of the Bar Association, though temporarily present during the search of the computer facilities, was mainly busy supervising the seizure of documents and could therefore not properly exercise his supervisory function as regards the electronic data. Second, the report setting out which search criteria had been applied and which files had been copied and seized was not drawn up at the end of the search but only later the same day. Moreover, the officers apparently left once they had finished their task without informing the first applicant or the representative of the Bar Association of the results of the search.
64. It is true that the first applicant could have requested, in a global manner at the beginning of the search, to have any disks with copied data sealed and submitted to the investigating judge. However, since the Code of Criminal Procedure provides for a report to be drawn up at the end of the search, and requires that the items seized be listed, he could expect that procedure to be followed. Since this was not the case he had no opportunity to exercise his rights effectively. Consequently, the Government's objection of non-exhaustion has to be dismissed.
65. With regard to the first applicant this manner of carrying out the search incurred the risk of impinging on his right to professional secrecy. The Court has attached particular weight to that risk since it may have repercussions on the proper administration of justice (see *Niemietz*, cited above, p. 36, § 37). The domestic authorities and the Government argued that the first applicant was not the applicant company's counsel and that the data seized did not concern their client-lawyer relationship. It is true that the first applicant, contrary to his submissions before the Court, did not claim before the domestic authorities that he was the applicant company's counsel, nor that he was the counsel of Novamed. However, he claimed throughout the proceedings that he acted as counsel for numerous companies whose shares were held by the second applicant. Moreover, the Government did not contest the applicants' assertion that the electronic data seized contained by and large the same information as the paper documents seized, some of which were returned to the first applicant by the investigating judge as being subject to professional secrecy. It can therefore be reasonably assumed that the electronic data seized also contained such information.
66. In conclusion, the Court finds that the police officers' failure to comply with some of the procedural safeguards designed to prevent any abuse or arbitrariness and to protect the lawyer's duty of professional secrecy rendered the search and seizure of the first applicant's electronic data disproportionate to the legitimate aim pursued.
67. Furthermore, the Court observes that a lawyer's duty of professional secrecy also serves to protect the client. Having regard to its above findings that the first applicant represented companies whose shares were held by the second applicant and that the data seized contained some information subject to professional secrecy, the Court sees no reason to come to a different conclusion as regards the second applicant.
68. Consequently, there has been a violation

of Article 8 in respect of both applicants.

II. Application of Article 41 of the Convention

69. Article 41 of the Convention provides:
"If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

70. Under the head of pecuniary damage, the first applicant claimed 4,000 euros (EUR) per year starting with the year 2000 for loss of clients. He submitted that he was unable to adduce proof without breaching his duty of professional secrecy. Moreover, he claimed EUR 10,000 as compensation for non-pecuniary damage since his reputation as a lawyer had suffered as a result of the events.
71. The applicant company claimed EUR 20,211.56 in compensation for pecuniary damage. It asserted that, being a holding company, its name had been ruined by the seizure of the data. Consequently, it had had to be newly established under another name and had therefore had to raise EUR 17,500 for the nominal capital of the new company and to pay costs of EUR 2,711.56 for the legal acts involved. It did not submit a claim in respect of non-pecuniary damage.
72. The Government asserted that there was no causal link between the violation at issue and the pecuniary damage alleged by the applicants.
73. With regard to the applicants' claims in respect of pecuniary damage, the Court observes that it cannot speculate as to what the effects on the applicants' reputation would have been had the search and seizure of electronic data been carried out in compliance with the requirements of Article 8 (see, *mutatis mutandis*, *Société Colas Est and Others*, cited above, § 54). Consequently, it makes no award under this head.
74. However, the Court accepts that the first applicant has suffered non-pecuniary damage, such as distress and frustration resulting from the manner in which the search and seizure of data were carried out. Making an assessment on an equitable basis and having regard to the sum awarded in a comparable case (see *Petri Sallinen and Others*, cited above, § 114) it grants the first applicant EUR 2,500 under the head of non-pecuniary damage.

B. Costs and expenses

75. The first applicant claimed a total amount of EUR 15,967.15 for costs and expenses, composed of EUR 9,204.52 in respect of the domestic proceedings and EUR 6,762.63 in respect of the Convention proceedings. These sums include value-added tax (VAT).
76. The Government accepted that the costs listed in respect of the domestic proceedings were necessarily incurred. However, they submitted that the amounts claimed were excessive since they were not in accordance with the relevant domestic laws and regulations on the remuneration of lawyers. In particular, only an amount of EUR 1,486.80 – instead of the EUR 4,858 claimed – was due in respect of the proceedings before the Salzburg Independent Administrative Panel. Moreover, the Government argued that the costs claimed in respect of the Convention proceedings were excessive. Only an amount of EUR 2,289.96 was appropriate.
77. The Court reiterates that if it finds that there has been a violation of the Convention, it may award the applicant the costs and expenses of the domestic proceedings which were necessarily incurred in order to prevent or redress the violation and are reasonable as to quantum (see *Société Colas Est and Others*, cited above, § 56).
78. The Court notes that it is not contested that the costs claimed by the first applicant were necessarily incurred. However, it considers that the sums claimed are not reasonable as to quantum. Regard being had to the information in its possession and to the sums awarded in comparable cases, the Court considers it reasonable to award the sum of EUR 10,000 covering costs under all heads. This sum includes VAT.

C. Default interest

79. The Court considers it appropriate that the default interest should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

For these reasons, the Court

1. *Dismisses* unanimously the Government's

preliminary objection as to non-exhaustion of domestic remedies;
2. *Holds* unanimously that there has been a violation of Article 8 of the Convention in respect of the first applicant;
2. *Holds* by four votes to three that there has been a violation of Article 8 of the Convention in respect of the second applicant;
3. *Holds* unanimously
(a) that the respondent State is to pay the first applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 2,500 (two thousand five hundred euros) in respect of non-pecuniary damage and EUR 10,000 (ten thousand euros) in respect of costs and expenses;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
4. *Dismisses* unanimously the remainder of the applicants' claim for just satisfaction.

Joint partly dissenting opinion of Judges Bratza, Casadevall and Mijović
While in full agreement that the first applicant's rights under Article 8 were violated in the present case, we take a different view as regards the second applicant.
Although the first applicant was the owner and general manager of the applicant company and although the company had its seat at the first applicant's law office, he was not the counsel or legal adviser of the company. It appears that the first applicant acted as legal adviser of certain of the companies owned by the second applicant. However, it has not been claimed that the search and seizure carried out in the first applicant's law office involved electronic data relating to any of the subsidiary companies of which he was the legal adviser. In these circumstances, we are not satisfied that the applicant company may be said to have been affected by the absence of procedural safeguards designed to protect the lawyer-client relationship which have been found by the Court to give rise to a finding of a violation of Article 8 of the Convention.

NOOT

1. Met deze uitspraak heeft het Hof op twee punten een verfijning aangebracht op zijn eerdere jurisprudentie over het beroepsgeheim van advocaten en de bescherming van 'private life' in het advocatenkantoor. Ten eerste geeft het Hof concreet aan welke waarborgen gelden bij strafrechtelijk onderzoek naar digitale bestanden en computersystemen in een advocatenkantoor. Ten tweede volgt uit deze uitspraak dat, indien er geen bijzondere wetgeving is voor strafrechtelijk onderzoek in een digitale omgeving, de nationaalrechtelijke normen die gelden voor onderzoek naar papieren documenten en administraties ook dienen te worden toegepast op digitale bestanden. In het onderstaande worden beide punten belicht.
2. De klacht van appellanten, de advocaat Wieser en de besloten vennootschap Bicos Beteiligungen GmbH (verder: Bicos), betreft het doorzoeken en in beslag nemen van digitale bestanden door de politie-functionarissen. Onder verwijzing naar *Niemietz t. Duitsland* (EHRM 16 december 1992, nr. 13710/88, *NJCM-Bulletin* 1993, p. 320, m.nt. EM, *NJ* 1993, nr. 400, m.nt. EJD) en *Petri Sallinen e.a. t. Finland* (EHRM 27 september 2005, nr. 50882/99) stelt het Hof voorop dat het doorzoeken en in beslag nemen van elektronische data een inbreuk vormt op art. 8 EVRM. Het Hof kwalificeert het advocatenkantoor van Wieser en het daarmee samenvallende bedrijfskantoor van Bicos daarbij als 'woning' in de zin van art. 8, eerste lid. Ook overweegt het Hof, eveneens in lijn met voornoemde jurisprudentie (zie *Niemietz*, reeds aangehaald, par. 32 en *Petri Sallinen*, par. 71) dat het doorzoeken en in beslag nemen van de digitale bestanden in het kantoor een inbreuk vormt op het recht op 'vertrouwelijke correspondentie' in de zin van deze bepaling. In het kader van de doeltoets stelt het Hof kortweg vast dat het doorzoeken en in beslag nemen van de data plaatsvond in het kader van een strafrechtelijk onderzoek naar illegale handel in medicijnen en dus een legitiem doel diende: het voorkomen van strafbare feiten.
3. Ten aanzien van de vraag of de inbreuk proportioneel was ten opzichte van het te bereiken doel toetst het Hof, onder verwijzing naar *Societé Colas Est e.a. t. Frankrijk* (EHRM

16 april 2002, nr. 37971/97, *EHRC* 2002/46, m.nt. H. Janssen, par. 48 e.v.) aan twee criteria. Ten eerste: is het onderzoek uitgevoerd op bevel van een rechter gebaseerd op een redelijke verdenking en beperkt in reikwijdte? En ten tweede, nu het onderzoek plaatsvindt in een advocatenkantoor: is het uitgevoerd in aanwezigheid van een onafhankelijke waarnemer om te voorkomen dat materialen die onder het beroepsgeheim vallen werden meegenomen?

4. Het Hof stelt vast dat in casu aan het eerstgenoemde criterium is voldaan. Het onderzoek is uitgevoerd op bevel van een onderzoeksrechter (de rechtbank te Salzburg) in het kader van een strafrechtelijk onderzoek naar illegale handel in medicijnen, gebaseerd op het feit dat facturen met de naam Novamed waren gevonden. Gelet hierop oordeelt het Hof dat het onderzoek in het kantoor van Wieser en Bicos is gebaseerd op een redelijke verdenking. Nu het onderzoek zich uitsluitend richtte op documenten die duidden op contacten met de van illegale handel in medicijnen verdachte personen, is ook aan de eis van een beperkte reikwijdte voldaan.

5. Aan het tweede criterium is naar het oordeel van het Hof echter niet voldaan. Weliswaar heeft het eerste politieteam, dat onderzoek deed naar de papieren administratie, de van toepassing zijnde normen van strafprocesrecht wel toegepast, maar het tweede politieteam, dat zich richtte op het computernetwerk van het kantoor, heeft deze regels niet in acht genomen. Het Oostenrijkse Wetboek van Strafvordering bevat onder meer de volgende waarborgen: de eis dat de gebruiker van het pand aanwezig is; de eis dat een verslag wordt opgesteld waarin de in beslag genomen objecten worden opgesomd; de regel dat, indien de eigenaar van het object bezwaar maakt, het document wordt verzegeld en een rechter beslist of het object wel of niet wordt gebruikt voor het onderzoek; en de eis dat, indien het een advocatenkantoor betreft, een vertegenwoordiger van de Orde van Advocaten aanwezig is. Terwijl deze normen bij het onderzoek naar de papieren administratie nauwgezet werden toegepast, werden zij bij het gelijktijdige digitale onderzoek genegeerd.

6. Het Hof beschrijft op gedetailleerde wijze hoe de twee onderzoeksteams te werk gingen. Uit deze overwegingen, en het daarop volgende oordeel van het Hof dat in casu niet aan de proportionaliteitstoets was voldaan, kunnen drie punten worden afgeleid. Ten eerste kan worden vastgesteld dat het Hof de lat voor strafrechtelijk onderzoek naar digitale bestanden even hoog legt als voor onderzoek naar papieren documenten. De Oostenrijkse regering heeft niet betwist dat de in beslag genomen – althans gekopieerde – digitale bestanden min of meer dezelfde informatie bevatten als de in beslag genomen papieren documenten. Sommige van de papieren documenten zijn later door de onderzoeksrechter teruggegeven (en dus niet betrokken in het strafrechtelijk onderzoek) omdat zij onder Wiesers beroepsgeheim als advocaat vielen. Aangenomen mag worden, zo merkt het Hof op, dat ook de in beslag genomen elektronische bestanden zulke vertrouwelijke informatie bevatten. Gelet op de ratio van de naar Oostenrijks recht geldende waarborgen is het mijns inziens logisch dat het Hof een verschil in beschermingsniveau bij papieren en digitaal onderzoek niet accepteert. In de tweede plaats kan worden geconcludeerd dat het niet uitmaakt of het nationale recht wel of geen bijzondere wettelijke normen voor digitaal onderzoek bevat (in dit geval kende het Oostenrijkse recht geen bijzondere bepalingen voor digitaal onderzoek: zie hierover par. 27-34 en 54 van de uitspraak). In het kader van de proportionaliteitstoets onderzoekt het Hof of het nationale recht voldoende en effectieve waarborgen biedt tegen misbruik en willekeur. Indien, zoals in dit geval, afzonderlijke wettelijke normen voor digitaal onderzoek ontbreken, zal het Hof toetsen of bij het doorzoeken en in beslag nemen van de digitale bestanden is voldaan aan de geldende normen voor onderzoek naar papieren documenten. In het onderhavige geval was er nog een extra complicatie. Doordat het onderzoek naar de papieren administratie en het computeronderzoek gelijktijdig plaatsvonden – hetgeen in de praktijk overigens zeer gangbaar is – kon de aanwezige vertegenwoordiger van de Orde van Advocaten niet op twee fronten tegelijk de bescherming bieden die hij werd geacht te bieden: voorkomen dat materialen die onder het beroepsgeheim van Wieser vielen, zouden worden meegenomen.

7. In deze zaak was het digitale onderzoek, evenals als het papieren onderzoek, overzichte-

lijk qua reikwijdte: het vond plaats *in* het kantoor van Wieser en Bicos en richtte zich – zo heeft het Hof vastgesteld – op een beperkt aantal 'zoektermen': woorden die duidden op contacten tussen Novamed en de van illegale handel in medicijnen verdachte personen. Kenmerkend voor digitaal onderzoek in bredere zin is evenwel juist dat het dikwijls zeer breed van opzet is. Dit hangt samen met de aard van de gebruikte technologieën (zie uitgebreid over de privacyrechtelijke aspecten van digitaal strafvorderlijk onderzoek, en in het bijzonder netwerkonderzoek op afstand, datamining en software-agents: R. Sietsma, *Gegevensverwerking in het kader van de opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy (*diss.*)*, Sdu Uitgevers: Den Haag 2006; B.W. Schermer, *Software agents, surveillance, and the right to privacy: a legistative framework for agent-enabled surveillance* (diss): Leiden University Press: Leiden 2007; H.P.G. Janssen en G.W.T.J. Michels, 'Politiegegevens', in: J.M.A. Berkvens en J.E.J. Prins, 'Privacyregulering in theorie en praktijk, Kluwer: Deventer 2007, p. 83-103). Ten eerste bieden de nieuwste ICT-toepassingen volop mogelijkheden om onderzoek op afstand te verrichten. Daarbij wordt via een dikwijls draadloze internetverbinding van buiten het fysieke kantoor (voor zover van een fysiek kantoor sprake is) toegang gezocht tot het te onderzoeken computernetwerk en kunnen aldus digitale bestanden worden doorzocht en gekopieerd zonder dat de beheerder van het netwerk dit merkt. Ten tweede zijn de mogelijkheden van digitale opsporingstechnieken, zoals datamining en zogeheten 'software-agents' (zie over de technische werking van 'agent-enabled surveillance' en de privacy- en strafrechtelijke aspecten hiervan Schermer 2007, reeds aangehaald, p. 17-34 en p. 71 e.v.), aanzienlijk groter dan de mogelijkheden van papieren onderzoek en kunnen de sporen van digitaal onderzoek relatief gemakkelijk worden uitgewist. Dit betekent dat het digitaal onderzoek, anders dan in de zaak *Wieser*, dikwijls breed en diepgaand qua opzet zal zijn en dat het voor rechters achteraf lastig is te controleren hoe breed en diepgaand het onderzoek daadwerkelijk is geweest. Een deel van de waarborgen voor het beroepsgeheim van advocaten en de vertrouwelijke correspondentie van bedrijven, waaraan het Hof blijkens deze uitspraak veel waarde hecht, kan bij deze nieuwste digitale opsporingsonderzoeken niet goed worden toegepast, of in elk geval gemakkelijk worden genegeerd. Dit betreft onder meer de norm dat een vertegenwoordiger van de Orde van Advocaten aanwezig is ten tijde van het onderzoek en de norm dat de documenten, alvorens in beslag te worden genomen (bij digitale documenten gaat het meestal om het kopiëren van data), aan de advocaat, respectievelijk de eigenaar of manager van de onderneming, worden getoond.

8. Voor de Verdragssluitende Partijen bij het EVRM brengt deze technologische ontwikkeling met zich mee dat zij zullen moeten onderzoeken of de nu geldende waarborgen voor strafrechtelijk onderzoek bij ondernemingen en advocatenkantoren, die vaak zijn ontwikkeld in het 'papieren tijdperk', zich lenen voor toepassing in een volledig digitale omgeving, en deze zonodig zullen moeten aanpassen of aanvullen, of ten minste zodanig interpreteren dat de ratio van de waarborgen ook in een digitale context wordt gegarandeerd. Voor het Hof betekent deze technologische ontwikkeling dat het een nieuwe invulling zal moeten geven aan het evenwicht tussen enerzijds het opsporingsbelang en anderzijds het belang van respect voor vertrouwelijke correspondentie van ondernemingen en private personen en het beroepsgeheim voor advocaten. Met deze uitspraak *Wieser* heeft het Hof het signaal afgegeven dat het zich bewust is van de risico's van digitaal opsporen voor het recht op vertrouwelijke correspondentie. Voor de nabije toekomst is het van belang dat het Hof zich rekenschap blijft geven van de vergaande mogelijkheden van de nieuwe opsporingstechnologieën en de grenzen zal aangeven voor het gebruik hiervan.

Marga Groothuis
Universitair docent staats- en bestuursrecht, Afdeling Staats- en Bestuursrecht, Universiteit Leiden