



COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

FOURTH SECTION

DECISION

AS TO THE ADMISSIBILITY OF

Application no. 74336/01
by Gottfried WIESER and BICOS Beteiligungen GmbH
against Austria

The European Court of Human Rights (Fourth Section), sitting on
16 May 2006 as a Chamber composed of:

Sir Nicolas BRATZA, *President*,

Mr J. CASADEVALL,

Mr G. BONELLO,

Mr M. PELLONPÄÄ,

Mr K. TRAJA,

Mrs E. STEINER,

Mr L. GARLICKI, *judges*,

and Mr M. O'BOYLE, *Section Registrar*,

Having regard to the above application lodged on 3 August 2001,

Having regard to the observations submitted by the respondent
Government and the observations in reply submitted by the applicants,

Having deliberated, decides as follows:

THE FACTS

The first applicant, Mr Gottfried Wieser, is an Austrian national who was born in 1949 and lives in Salzburg. The second applicant, BICOS Beteiligungen GmbH, is a limited liability company with its seat in Salzburg. They are represented before the Court by Ms P. Patzelt, a lawyer practising in Salzburg. The Austrian Government ("the Government") are represented by their Agent, Ambassador F. Trauttmansdorff, Head of the International Law Department at the Federal Ministry of Foreign Affairs.

A. The circumstances of the case

The facts of the case, as submitted by the parties, may be summarised as follows.

The first applicant is a lawyer practising in Salzburg. He is the owner and general manager of the second applicant (“applicant company”), a holding company which is, *inter alia*, the owner of the NOVAMED limited liability company.

On 30 August 2000 the Salzburg Regional Court (*Landesgericht*), upon a request for mutual assistance (*Rechtshilfeersuchen*) by the Naples Public Prosecutor’s Office, issued a warrant to search the seat of the applicant company and the NOVAMED company. Both companies have their seats at the first applicant’s law office.

The court noted that in the course of pending criminal proceedings concerning, *inter alia* illegal trade with medicaments against a number of persons and companies in Italy, invoices addressed to the NOVAMED company, owned as to 100% by the applicant company, had been found. It therefore ordered the seizure of all business documents revealing contacts with the suspected persons and companies.

1. The search of the applicants’ premises and seizure of documents and data

On 10 October 2000 the search of the seat of the applicant company, which is at the same time the first applicant’s law office, was carried out by 8 to 10 officers of the Salzburg Economic Police (*Wirtschaftspolizei*) and data securing experts (*Datensicherungsexperten*) of the Federal Ministry for the Interior.

One group of the officers searched the law office for files concerning “NOVAMED” or “BICOS” in the presence of the first applicant and a representative of the Salzburg Bar Association. All documents were shown to the first applicant and the representative of the Bar Association before seizure.

Whenever the first applicant objected to an immediate examination of a document seized it was sealed and deposited at the Salzburg Regional Court as required by Article 145 of the Code of Criminal Procedure (*Strafprozeßordnung* - see below). All seized or sealed documents were listed in a search report which was signed by the applicant and the officers who had carried out the search.

Simultaneously, another group of officers examined the first applicant’s computer facilities and copied several data files to disks. According to his statement before the Independent Administrative Panel (see below) the IT specialist servicing the computer facilities was called to provide some technical assistance but left again after about half an hour. The

representative of the Bar Association was informed about the search of the computer facilities and was also temporarily present. When the officers had terminated the search of the computer facilities, they left without having drawn up a search report and, apparently, also without informing the first applicant about the results of the search.

Later on the same day the police officers involved in the search of the applicants' electronic data drew up a data securing report (*Datensicherungsbericht*). Apart from a number of technical details concerning the first applicant's computer facilities, the report states that no complete copy of the server was made. The search was carried out with the names of the companies involved and with the names of the suspects in the Italian proceedings. A folder named NOVAMED containing 90 files was found plus one further file containing one of the search items. All these data were copied to disks. In addition the deleted items were reactivated and numerous files which corresponded to the search items were found and also copied to disks.

On 13 October 2000 the investigating judge opened the sealed documents in presence of the first applicant. Some documents were copied and taken to the file while others were returned to the first applicant on the ground that their use would impinge on the first applicant's duty of professional secrecy.

As regards the disks with the secured data, they were transmitted to the Economic Police where all files were printed out. Both, the discs and print-outs were then handed over to the investigating judge.

2. The applicants' complaint to the Review Chamber

On 28 November 2000 the first applicant, and on 11 December 2000 the applicant company, lodged complaints with the Review Chamber (*Ratskammer*) of the Salzburg Regional Court (*Landesgericht*).

They submitted that the first applicant was the owner and manager of the applicant company but also the lawyer of a number of companies in which the latter held shares. They complained that the search of their premises and the seizure of electronic data had infringed the first applicant's right and duty to professional secrecy under Section 9 of the Lawyer's Act (*Rechtsanwaltsordnung*) in conjunction with Article 152 of the Code of Criminal Procedure as some officers had proceeded unobserved to an examination and subsequent copying of electronic data. The applicants submitted that these data contained the same information as the documents which had been examined in the presence of the first applicant. However, with regard to the electronic data, the first applicant had not been given an opportunity to object and have the disks sealed.

They further submitted that the search report did not mention these proceedings nor did it mention which electronic data had been copied and seized. Furthermore, the search report, which was only signed by three of

the officers, did not mention the names of all the officers who had been present at the search, omitting in particular the names of the data securing experts.

On 31 January 2001 the Review Chamber dismissed the applicants' complaints.

It observed that the first applicant's computer data had been searched with the aid of particular search criteria. Data files which corresponded to these search criteria had been copied to disks which had been seized.

However, there was no ground for holding that this seizure circumvented Article 152 of the Code of Criminal Procedure: the search of the first applicant's law office concerned exclusively documents which the first applicant had in his possession as an organ of the NOVAMED and BICOS companies, respectively, and therefore did not concern a lawyer-client relationship.

It further observed that the search of the first applicant's law office was based on a lawful search warrant which included the search and seizure of electronic data. The procedural safeguards laid down in Article 145 of the Code of Criminal Procedure, namely the right of the person concerned to object to an immediate examination and to request the deposit of data seized with the Regional Court and a decision by the Review Chamber, also applied to the search of electronic data.

In the present case, however, the officers had, whenever asked, complied with the first applicant's requests to seal certain documents and deposit them with the Regional Court. Some of these documents had been returned by the court in order to ensure compliance with the applicant's duty of professional secrecy.

It therefore concluded that the applicants' complaints were unfounded. The Review Chamber's decision was served on 7 February 2001.

3. The applicants' complaint to the Salzburg Independent Administrative Panel

In the meantime, on 20 November and on 21 November 2000, respectively, the applicants lodged complaints with the Salzburg Independent Administrative Panel (*Unabhängiger Verwaltungssenat*). They submitted that the search and seizure of electronic data in the first applicant's office had been unlawful.

On 2 April 2001, on 11 June 2001 and on 11 July 2001 the Independent Administrative Panel held public hearings at which it heard a number of witnesses.

The IT specialist in charge of the first applicant's computer facilities said that he had been called and had arrived at the office when the search of the premises was already underway. He had left again after half an hour. The officer in charge of the search stated that the first applicant had been informed about the search of his computer data. Two other officers stated

that the search of the first applicant's computer facilities had not been started until the arrival of his IT specialist and that the representative of the Bar Association had been temporarily present. This was confirmed by the representative of the Bar Association.

On 24 October 2001 the Independent Administrative Panel (*Unabhängiger Verwaltungssenat*) rejected the applicants' complaints. It found that the applicants' complaints concerned alleged breaches of certain provisions of the Code of Criminal Procedure regulating a search. The officers who had carried out the search had possibly not entirely respected these provisions. They had, however, acted on the basis of the search warrant and not exceeded the instructions of the investigating judge. The search was therefore attributable to the court. Consequently, a review of lawfulness did not fall within the competence of the Independent Administrative Panel.

B. Relevant domestic law and practice

1. Provisions of the Code of Criminal Procedure relating to search and seizure

Articles 139 to 149 of the Code of Criminal Procedure (*Strafprozeßordnung*) concern the search of premises and persons and the seizure of objects.

Article 139 § 1 provides in particular that a search may only be carried out if there is a reasonable suspicion that in the premises concerned a person suspected of having committed an offence is hiding, or that there are objects, the possession or examination of which is relevant for a particular criminal investigation.

According to Article 140 §§ 1 and 2, a search should in general only be carried out after the person concerned has been heard, and only if the person or objects searched for have not been voluntarily produced and if the reasons leading to the search have not been eliminated. It is not required to have such a hearing where there is danger in delay.

Article 140 § 3 states that a search may, as a rule, only be carried out on the basis of a reasoned search warrant issued by a judge.

Pursuant to Article 142 §§ 2 and 3 the occupant of the premises subject to the search or, if he is unavailable, a relative of the occupant shall be present during the search. A report is to be drawn up and to be signed by all those present.

Article 143 § 1 of the Code of Criminal Procedure provides that, if objects relevant for the investigations or subject to forfeiture or confiscation are found, they are to be listed and taken into safekeeping at the court or to be seized. It refers, in this respect, to Article 98 according to which objects

in safe-keeping have to be put into an envelope to be sealed by the court, or to have a label attached so as to avoid any substitution or confusion.

Article 145 reads as follows:

“1. When searching through documents steps must be taken to ensure that their content does not become known to unauthorised persons.

2. If the owner of the documents does not want to permit their search, they shall be sealed and deposited with the court; the Review Chamber must determine immediately whether they are to be examined or returned.”

According to the courts’ case-law which is endorsed by the opinion of academic writers (see, *Bertl/Vernier, Grundriss des österreichischen Strafprozessrechts*, 7th edition), the provisions relevant to the search and seizure of paper documents also apply *mutatis mutandis* to the search and seizure of electronic data. If the owner of disks or hard disks on which data are stored objects to their search, the data carriers are to be sealed and the Review Chamber has to decide whether they may be examined.

2. Provisions relating to the professional secrecy of lawyers

Section 9 of the Austrian Lawyers’ Act (*Rechtsanwaltsordnung*) regulates the professional duties of lawyers including, *inter alia*, the duty to keep professional secrecy.

Article 152 § 1 of the Code of Criminal Procedure exempts lawyers, notaries and business trustees from the obligation to give evidence as witnesses in respect of information given to them in the exercise of their profession.

It is established case-law that documents which contain information subject to professional secrecy may not be seized and used in a criminal investigation.

According to an instruction (*Erlaß*) of the Federal Minister of Justice of 21 July 1972, a representative of the competent Bar Association may be present during the search of a lawyer’s office in order to ensure that the search does not encroach on professional secrecy.

3. Review by the Independent Administrative Panel

By virtue of Section 67a § 1 of the General Administrative Procedure Act (*Allgemeines Verwaltungsverfahrensgesetz*), Independent Administrative Panels have jurisdiction, *inter alia*, to examine complaints from persons alleging a violation of their rights resulting from the exercise of direct administrative authority and coercion (*Ausübung unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt*).

Where police officers execute a court warrant their acts are imputable to the court unless they act in clear excess of the powers conferred on them. Only in the latter case their acts are qualified as exercise of direct

administrative authority and coercion and are subject to review by the Independent Administrative Panel.

COMPLAINT

The applicants complain under Article 8 of the Convention about the search and seizure of electronic data carried out in the context of a search of their premises. They submit that the officers acted in breach of the first applicant's right and duty of professional secrecy as computer data was searched for and subsequently seized without his knowledge and without respecting the necessary procedural safeguards.

THE LAW

The applicants complain about the search and seizure of electronic data. They rely on Article 8 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.”

The Government contended in the first place that the applicants have failed to exhaust domestic remedies. They argued in particular that Article 145 § 2 of the Code of Criminal Procedure applied also to the search of electronic documents. If their owner did not want to permit the search, the data carriers were to be sealed and deposited with the court and it was then for the Review Chamber to decide whether the data might be examined or was to be returned. This kind of judicial review provided an effective remedy.

However, the first applicant did not make any request to seal the copied data. In this connection, the Government contested the first applicant's claim that he was not aware of the search of his computer facilities and the seizure of data. They observed that his computer specialist was called and that the representative of the bar association was informed in detail about the steps taken by the officials who copied the data.

The applicants contested that the first applicant had failed to request that the seized data be sealed. On the contrary, the way in which the search was carried out deprived him of the possibility to make use of his rights. The search of his computer facilities was carried out at the same time as the

search of his paper files, he was not informed what kind of data had been copied and seized and no report was drawn up before the officers left his premises. He was therefore not in a position to request that data be sealed in order to obtain a ruling by the Review Chamber on whether they could be used for the investigation or not.

The Court considers that in the circumstances of the present case the issue of exhaustion of domestic remedies is closely linked to the issue of compliance with Article 8 and should therefore be joined to the merits.

In the alternative, the Government argued that, assuming that the search of the first applicant's law office which was at the same time the seat of the applicant company constituted an interference with their private life and home, this interference was justified under Article 8 § 2 of the Convention.

They 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 remained unsubstantiated as regards the applicant company.

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.

As regards the necessity of the interference, the Government asserted that the search and seizure of data was proportionate to the legitimate aim pursued. The contested measures had been ordered by a judicial search warrant which delimited their scope. Moreover, Austrian law contained specific procedural safeguards for the search of a lawyer's office. They were complied with in that the search took place in presence of the applicant and a representative of the Bar Association, whose role was 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 were searched with the help of certain key words, i.e. 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 was not affected. Moreover, the representative of the Bar association was informed of the search of the first applicant's computer facilities and the modalities of the search were documented in the data securing report. The fact that the said report was not drawn up during the search but later the same day was not decisive since the main aim of laying down which data had been seized had been achieved.

For their part the applicants asserted that the search and seizure of electronic data was disproportionate. They pointed out that the first applicant was not only the manager of the applicant company but also its counsel and the counsel of the NOVAMED company. Thus the search

necessarily led to correspondence, for instance to 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 they had been sealed and returned to the applicant by the investigating judge as being protected by professional secrecy. In contrast, the electronic data had been seized without observing the attending procedural guarantees. In this connection the applicants relied on the same arguments as submitted in respect of the issue of exhaustion of domestic remedies.

The applicants maintained that the applicant company's rights were also infringed, since it had no control over the kind of data that were seized. The search for the word BICOS necessarily led to data unrelated to the subject defined in the search warrant. The procedural guarantees laid down in the Code of Criminal Procedure were not complied with since the applicant company was not 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.

The Court considers, in the light of the parties' submissions, that the application raises serious issues of fact and law under the Convention, the determination of which requires an examination of the merits. The Court concludes therefore that the application is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. No other ground for declaring it inadmissible has been established.

For these reasons, the Court unanimously

Declares the application admissible, without prejudging the merits of the case.

Michael O'BOYLE
Registrar

Nicolas BRATZA
President