

## 1. Internationales Strafrecht, EMRK und Verfassungsrecht Droit pénal international, CEDH et droit constitutionnel

**Nr. 41** EGMR, Fourth Section, Case of Wieser and Bicos Beteiligungen GmbH v. Austria vom 16. Oktober 2007 – Application no. 74336/01

### Art. 8 EMRK: Schutz des Privatlebens, Durchsuchung einer Anwaltskanzlei.

Der Begriff «law» in Art. 8 Abs. 2 EMRK umfasst das geltende Recht, wie es von den zuständigen Gerichten ausgelegt wird. Nationale Vorschriften über die Beschlagnahme und Durchsuchung von Gegenständen und Papieren können auch die Beschlagnahme und Durchsuchung elektronischer Daten legitimieren, wenn eine erweiternde Auslegung durch die nationale Rechtspraxis anerkannt ist. Dabei müssen jedoch die für derartige Eingriffe vorgesehenen Schutzmechanismen vollumfänglich beachtet werden (§§ 53 ff.). (Regeste forumpoenale)

### Art. 8 CEDH: protection de la vie privée, perquisition dans une étude d'avocat.

La notion de «loi» figurant à l'art. 8 al. 2 CEDH recouvre le droit positif tel qu'il est interprété par les tribunaux compétents. Les dispositions du droit national sur la saisie et la perquisition d'objets et de documents permettent de légitimer la saisie et la perquisition de données électroniques si la pratique interne admet une interprétation extensive. En pareille hypothèse, les mécanismes de protection prévus pour ce genre d'atteintes doivent toutefois être pleinement observés (§§ 53 ss.). (Résumé forumpoenale)

### Art. 8 CEDU: protezione della vita privata, perquisizione di uno studio legale.

La nozione di «law» nell'art. 8 cpv. 2 CEDU comprende il diritto vigente come viene interpretato dai tribunali competenti. Le disposizioni del diritto nazionale concernenti il sequestro e la perquisizione di oggetti e di documenti permettono di legittimare il sequestro e la perquisizione di dati elettronici se la giurisprudenza nazionale ammette un'interpretazione estensiva. I meccanismi protettivi previsti per le ingerenze di questo tipo devono essere rispettati pienamente (§§ 53 segg.). (Regesto forumpoenale)

### Sachverhalt:

Der Beschwerdeführer zu 1) ist Anwalt mit Kanzleisitz in Salzburg. Weiterhin ist der Beschwerdeführer zu 1) Generalmanager der Beschwerdeführerin zu 2), der Bicos Beteiligungen GmbH, die wiederum alleinige Eigentümerin der Firma Novamed ist. Beide Unternehmen haben ihren Sitz in der Anwaltskanzlei des Beschwerdeführers zu 1). Auf ein Rechtshilfeersuchen italienischer Strafverfolgungsbehörden hin ordnete das Landgericht Salzburg die Durchsuchung des Sitzes der Bicos Beteiligungen GmbH und der Firma Novamed an. Die Durchsuchung wurde von Beamten der Wirtschaftspolizei unter Beizug von Datensicherungsexperten des Innenministeriums durchgeführt, die in zwei Gruppen agierten.

Eine erste Gruppe durchsuchte die Räumlichkeiten der Anwaltskanzlei nach Dokumenten, die im Zusammenhang mit der Bicos Beteiligungen GmbH und/oder der Firma Novamed standen. Die Durchsuchung erfolgte insoweit durchgängig in Anwesenheit des Beschwerdeführers zu 1) sowie eines Vertreters der Rechtsanwaltskammer. Alle Dokumente, die sichergestellt werden sollten, wurden dem Beschwerdeführer zu 1) und dem Vertreter der Rechtsanwaltskammer vorgelegt. Dokumente, deren Sicherstellung der Beschwerdeführer zu 1) widersprach, wurden versiegelt und so dem Untersuchungsrichter übergeben. Dieser entsiegelte sie einige Tage später in Anwesenheit des Beschwerdeführers zu 1) und entschied darüber, welche Dokumente zu beschlagnahmen seien.

Zeitgleich mit der ersten Gruppe durchsuchte eine zweite Gruppe von Beamten die Computeranlage des Beschwerdeführers zu 1) nach Dateien, die in Zusammenhang mit der Bicos Beteiligungen GmbH oder der Novamed stehen. Der Vertreter der Rechtsanwaltskammer und der für die Unterhaltung der Computeranlage des Beschwerdeführers zu 1) zuständige IT-Spezialist waren während dieser Durchsuchung lediglich zeitweise anwesend. Die Beamten sicherten Kopien der Dateien, welche die Suchkriterien erfüllten, auf einer Diskette. Die Diskette wurde der Wirtschaftspolizei übergeben, welche die Dateien ausdrückte und die Ausdrucke nebst der Diskette dem Untersuchungsrichter übergab. Weder wurde der Beschwerdeführer zu 1) im Anschluss an die Durchsuchung darüber informiert, welche Dateien kopiert worden waren, noch gibt der im Anschluss an die Durchsuchung erstellte Datensicherungsbericht detaillierte Auskunft darüber, welche Dateien im Einzelnen kopiert worden sind.

Rechtsmittel, mit denen die Beschwerdeführer gegenüber den nationalen Gerichten geltend gemacht hatten, dass die Sicherstellung der elektronischen Daten unter Verletzung der sich aus dem Anwaltsgeheimnis ergebenden Restriktionen erfolgt sei, blieben erfolglos. Der Gerichtshof bejaht eine Verletzung des Art. 8 EMRK.

### Aus den Erwägungen:

[...]

34. 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 is stored objects to their being searched, the data carriers are to be sealed and the Review Chamber must decide whether they may be examined.

[...]

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. Finland*, 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.

[...]

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.

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.

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 whether 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 Govern-

ment 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.

### **Bemerkungen:**

Der vorliegende Fall zeigt deutlich die besonderen Gefahren, die aus einer Vermischung der anwaltlichen Tätigkeit mit einer sonstigen wirtschaftlichen Aktivität resultieren. Bei Ermittlungen gegen Unternehmen sind Durchsuchungen am Firmensitz nichts Ungewöhnliches. Werden dabei wie im vorliegenden Fall die Sphären berufsspezifisch anwaltlicher und sonstiger wirtschaftlicher Tätigkeit räumlich nicht getrennt, sind Informationen der Mandanten des betreffenden Rechtsanwaltes dem erhöhten Risiko ausgesetzt, staatlichen Stellen bekannt zu werden. Obwohl der Erfolg der Beschwerde hier anderes suggeriert, nivelliert, wie unter I. aufzuzeigen sein wird, eine solche Vermischung der Tätigkeiten die sonst für die Ermittlungsbehörden zu überwindenden Hürden für die Durchsuchung einer Anwaltskanzlei.

Der Entscheid enthält zwei wesentliche Problemkreise. Dies ist zum einen die Frage der Übertragung der Beschlagnahmenvorschriften auf elektronische Daten (nachfolgend unter I.) und zum anderen die Problematik des Schutzes von Unterlagen beim Anwalt (vgl. unten II.).

I. Während im realen Leben immer mehr Geschäftsunterlagen elektronisch gespeichert werden und schriftliche Kommunikation auf elektronischem Wege erfolgt, befindet sich der Wortlaut einzelner nationaler Prozessordnungen mit ihren Vorschriften zur Beschlagnahme von Papieren immer noch im 19. Jahrhundert. Die entsprechende nationale Rechtsprechung hat hier oftmals weit schneller als der Gesetzgeber auf die Lebenswirklichkeit und die daraus resultierenden Bedürfnisse der Strafverfolgungsbehörden reagiert. Sie hat vielfach die Vorschriften zur Papierbeschlagnahme ergänzend ausgelegt und dahingehend interpretiert, dass der Papierbegriff der strafprozessualen Durchsuchungs- und Beschlagnahmeregeln auch elektronische Daten umfasst. Dies gilt nicht nur für das im vorliegenden Fall relevante österreichische Recht (vgl. oben § 54), sondern auch für die Schweiz (vgl. z.B. §§ 99 ff. ZH-StPO und hierzu SCHMID, Strafprozessrecht, 2. Aufl., Zürich 2004, N. 734; AEPLI, Die Strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, 2004, passim.) und für Deutschland (vgl. jetzt aber § 110 Abs. 3 dStPO, BGBl I. 2007, 3204; WOHLERS, in: Systematischer Kommentar zur Strafprozessordnung, 56. Lfg. [Februar 2008], § 110 N 8 ff.; zur alten Rechtslage vgl. BVerfGE 113, 29 ff.).

Der EGMR lässt in der vorliegenden Entscheidung diese auf elektronische Daten erweiternde Auslegung der überkommenen Sicherstellungsvorschriften für Papiere im Rahmen des Art. 8 EMRK genügen. Nach seiner Auffassung ist der Begriff «law» in Art. 8 Abs. 2 EMRK nicht im formellen, sondern im materiellen Sinne («substantive sense») zu verstehen, womit dann auch die Auslegung des nationalen Rechts durch die Gerichte erfasst ist. Einer ausdrücklichen formalesetzlichen Regelung, wie diese mit der neuen Beschlagnahmenvorschrift des Art. 245 der kommenden schweizerischen StPO entstehen wird (vgl. Botschaft BBl 2007, 1238), bedarf es daher mit Blick auf die EMRK nicht zwingend.

Entscheidend für den Erfolg der Beschwerde beider Beschwerdeführer war vorliegend die Nichtbeachtung der existierenden nationalen Schutzvorschriften (Anwesenheit eines Mitglieds der Anwaltskammer bei der Durchsuchung, Versiegelung sichergestellter Dokumente, Erstellung eines Sicherstellungsverzeichnisses). So verweist die Vierte Sektion des Gerichtshofes ausdrücklich darauf, dass diese Schutzvorschriften im vorliegenden Fall im Hinblick auf die beschlagnahmten Papiere eingehalten worden sind, während die untersuchenden Beamten dies bei den elektronischen Daten nicht getan haben (vgl. oben § 63). So war anlässlich der Durchsuchung der Computer das Mitglied der Anwaltskammer nicht immer anwesend, weil es mit der Überwachung der Durchsicht der Papiere beschäftigt war, der Bericht über die kopierten Dateien wurde nicht mit Abschluss der Sicherstellung übergeben und der Beschwerdeführer und das Mitglied der Anwaltskammer wurden über die Beendigung der Suche im Computersystem nicht informiert. Im Ergebnis bedeutet dies, dass das Gericht zwar eine Anpassung der be-

stehenden gesetzlichen Eingriffsbefugnisse an geänderte Lebenssachverhalte im Wege einer Auslegung für konventionskonform erachtet, andererseits aber fordert, dass die mit den auszulegenden Eingriffsbefugnissen korrespondierenden prozeduralen Schutzmechanismen damit nicht gleichzeitig einer Anpassung an Zweckmässigkeitsgesichtspunkte erfahren dürfen, sondern weiterhin Beachtung finden müssen.

Dem ist im Grundsatz zuzustimmen. Den prozeduralen Schutzmechanismen liegt letztlich eine gesetzgeberische Abwägung zwischen den Strafverfolgungsinteressen auf der einen Seite und entgegenstehenden Interessen, wie dem Schutz der Privatsphäre, des Familienlebens oder besonderer Berufsgruppen auf der anderen Seite zugrunde. Dürfte man im Wege der *erweiternden* Auslegung der Eingriffsbefugnisse diese bestehenden prozeduralen Schutzmechanismen einschränkend *auslegen*, würde man letztlich ihrer Natur nach neue Eingriffsbefugnisse schaffen: Neben der Eingriffsbreite würde auch die Eingriffstiefe und die Verortung in der Gesamtrechtsordnung modifiziert. Eine solche Entscheidung muss aber in einem auf Gewaltenteilung angelegten Staatswesen dem Gesetzgeber vorbehalten sein.

Zuzugeben ist, dass sich bei einer Datenbeschlagnahme, insbesondere bei grossen Datenmengen, erhebliche praktische Probleme stellen. So kann es aus forensischen Gründen notwendig sein, den gesamten Datenbestand zur Auswertung mitzunehmen, wenn diese vor Ort nicht möglich ist, weil z.B. eine Suche nach gelöschten, aber möglicherweise beweisrelevanten Daten vor Ort nicht ausgeführt werden kann. Indessen sind diese Probleme rein praktischer Natur und als solche auch lösbar. Dass hier im vorliegenden Verfahren zumindest ansatzweise versucht worden ist, eine adäquate Lösung zu finden und die Eingriffstiefe und den Eingriffsumfang zu begrenzen, zeigt die Vorgehensweise der ermittelnden Beamten, die anstatt den gesamten Datenbestand zu beschlagnahmen, mittels *spezifischer* Suchbegriffe eine Auswertung bereits vor Ort durchführten. Selbst wenn man aber solche Modifikation prozeduraler Schutzmechanismen *qua Natur der Sache* für zulässig hält, bleibt immer noch unverständlich, wieso im vorliegenden Verfahren die Beamten die vorhandenen Schutzregelungen wie die Anwesenheitsregelung, die Versiegelung und die Erstellung eines Verzeichnisses im Hinblick auf die Daten nicht eingehalten haben.

II. Besondere Probleme stellen sich immer dann, wenn Anwaltskanzleien Objekte einer Durchsuchung sind. Hier ist regelmässig nicht nur der unmittelbare Adressat von der Durchsuchungsmassnahme betroffen, sondern daneben zumindest potentiell immer auch eine Vielzahl Unbeteiligter – die Mandanten –, von deren Unterlagen bei der Durchsuchung Kenntnis genommen werden kann.

Der EGMR hat in seiner Rechtsprechung die besondere Bedeutung des Anwaltsgeheimnisses bei der Prüfung der Verhältnismässigkeit des Eingriffes betont (vgl. EGMR v. 16.12.1992, *Niemietz v. Deutschland*, Serie A, Nr. 251 B,

§§ 29 ff.). Eine wirksame Rechtsvertretung kann nur dann erfolgen, wenn der Mandant dem Rechtsanwalt alle relevanten Umstände seines Falles darlegen kann. Dies wird er aber nur dann tun, wenn er sich sicher ist, dass insbesondere für ihn nachteilige Umstände nicht privaten Dritten oder dem Staat zur Kenntnis gelangen. Der Rechtsanwaltsberuf ist somit nur denkbar, wenn auch der Staat diese Vertrauenssphäre grundsätzlich achtet. Jede Durchsuchung, die auch Informationen Dritter aus dieser Sphäre herausgelangen lässt, gefährdet dieses Vertrauen des Mandanten in die Sicherheit von Informationen bei einem Anwalt und damit die Effektivität der Rechtsvertretung. Fehlt es aber an einer wirksamen Rechtsvertretung, ist gleichzeitig eine notwendige Voraussetzung für die effektive Wahrnehmung der durch Art. 6 EMRK geschützten Rechte nicht mehr gewährleistet (EGMR, *Niemietz v. Deutschland*, § 37). Damit betrifft die Durchsuchung einer Anwaltskanzlei regelmässig mittelbar auch ein zweites, wichtiges Menschenrecht und verleiht dem Eingriff eine Schwere, die über dem einer Durchsuchung liegt, die allein an Art. 8 EMRK zu messen wäre.

Typischerweise kommt eine Durchsuchung von Anwaltskanzleien in zwei Konstellationen vor. Dies ist zunächst der Fall des Vorgehens gegen den Anwalt als Beschuldigten. Eine zweite Konstellation ist die, dass in einem gegen einen Mandanten geführten Verfahren die Kanzlei des Rechtsanwalts durchsucht wird. Untypisch ist hingegen eine Konstellation wie die hier vorliegende, bei der die Durchsuchung einer Anwaltskanzlei in einem Strafverfahren erfolgt, das sich weder gegen den Anwalt selbst noch gegen einen seiner Mandanten richtet. Zwar hatte der Beschwerdeführer zu 1) behauptet, dass die Beschwerdeführerin zu 2) seine Mandantin sei. Merkwürdigerweise hatte er diese Behauptung aber nicht schon im nationalen Verfahren, sondern erst vor dem Gerichtshof aufgestellt, was die Sektion dann veranlasste, dieses Vorbringen letztlich dahinstehen zu lassen (vgl. oben § 65). Vor diesem Hintergrund hätte es nun nahe gelegen, eine spezifische, aus dem Eingriff in das Anwaltsgeheimnis resultierende Betroffenheit der Beschwerdeführerin zu 2) zu verneinen. Die Vierte Sektion hat dies indes nicht getan, sondern eine Betroffenheit der Beschwerdeführerin zu 2) mit der Erwägung bejaht, dass der Beschwerdeführer zu 1) «acted as counsel for numerous companies whose shares were held by the second applicant» (vgl. oben § 65). Dass bei Kapitalgesellschaften allein schon das Bestehen einer Mandantenbeziehung zu den Töchtern eine *unmittelbare* Betroffenheit der Holding zur Folge haben soll (vgl. oben § 69), überzeugt nun aber nicht ohne weiteres. Warum eine hypothetische Gefährdung der Anwalt-Mandant-Beziehung bei einer Tochtergesellschaft eine Verletzung der Holding als selbständige juristische Person in eigenen Rechten begründen soll, bleibt dunkel. Während die Mehrheit des Gerichtshofs offenbar schon die abstrakte/potentielle Gefährdung der Mandanteninteressen ausreichen las-

sen will, gehen drei Richter – sachlich wohl eher überzeugend – davon aus, dass die Rechte der Beschwerdeführerin zu 2) nicht verletzt wurden:

«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.» (Joint partly dissenting opinion of Judges BRATZA, CASADEVALL and MIJOVIC)

Assess. iur. Stephan Schlegel, wissenschaftlicher Assistent und Doktorand an der Universität Zürich ■