# RECHTSPRECHUNG

## EGMR: Überwachung von privater E-Mail- und Internetnutzung am Arbeitsplatz – Copland vs. Vereinigtes Königreich

EMRK Art. 8, 41; Further and Higher Education Act 1992 (UK) Sec. 19
Urteil vom 3.4.2007 – Application no. 62617/00

**Leitsätze der Redaktion**

**1. Der Schutzbereich von Art. 8 Abs. 1 EMRK erfasst mit der Achtung von Privatleben und Korrespondenz auch die Nutzung von E-Mail und Internet am Arbeitsplatz. Das gilt auch für die Überwachung von Verkehrsdaten.**

**2. Ein Eingriff in das Grundrecht ist nicht i.S.v. Art. 8 Abs. 2 EMRK „gesetzlich vorgesehen", wenn eine Körperschaft öffentlichen Rechts – hier ein College – zwar über eine allgemeine Rechtssetzungsbefugnis zur Erfüllung ihrer gesetzlichen Aufgaben verfügt, hiervon jedoch hinsichtlich der Überwachung des Kommunikationsverhaltens ihrer Mitarbeiter keinen Gebrauch gemacht hat.**

**3. Auf Grund dessen bedarf es im vorliegenden Fall keiner Entscheidung, unter welchen Voraussetzungen eine derartige Überwachung im Einzelfall den weiteren Anforderungen von Art. 8 Abs. 2 EMRK – insbesondere hinsichtlich der Bestimmtheit der Ermächtigungsgrundlage – genügt.**

**Anm. d. Red.:** Die Leitsätze wurden verfasst von *Dr. Gerrit Hornung*, LL.M. (European Law), Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel.

**Sachverhalt**

Die Bf. war seit 1991 Angestellte des Carmarthenshire College, einer Körperschaft öffentlichen Rechts. Seit 1995 war sie persönliche Assistentin des Direktors und arbeitete eng mit dessen Stellvertreter zusammen. Auf Veranlassung des Stellvertreters wurden 1998 die Telefon-, Internet- und E-Mail-Nutzungen der Bf. überwacht; nach der Begründung des Bg. erfolgte dies, um zu klären, ob eine übermäßige Privatnutzung vorlag. Unstreitig wurden dabei die gewählten Telefonnummern, Zeitpunkt und Dauer der Gespräche und Kosten analysiert, nach Behauptung der Bf. auch eingehende Anrufe mit Gesprächspartnern und deren Dauer. Bei der Internetnutzung wurden die besuchten Webseiten mit Zeitpunkt und Nutzungsdauer aufgezeichnet, beim E-Mail-Verkehr die Adressen der Kommunikationspartner sowie der Zeitpunkt der Kommunikation. Die genaue Dauer der Maßnahmen blieb im Verfahren umstritten, betrug aber jedenfalls mehrere Monate.

Zum Zeitpunkt der Überwachungsmaßnahme gab es im Vereinigten Königreich keine gesetzliche Ermächtigungsgrundlage für die Überwachung der Kommunikation von Arbeitnehmern. Entsprechende Normen (Regulation of Investigatory Powers Act 2000 und Telecommunications (Lawful Business Practice) Regulations 2000) traten erst später in Kraft. Das College selbst verfügte über eine interne Regelungskompetenz, hatte aber keine Satzung oder ähnliche Regularien zur Aufzeichnung des Nutzungsverhaltens bei Telefon-, Internet- und E-Mail-Zugängen erlassen.

**Aus den Gründen**

*... I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION*

**29.** The applicant alleged that the monitoring activity that took place amounted to an interference with her right to respect for private life and correspondence under Art. 8 ...

**30.** The Government contested that argument.

**A. The parties' submissions**

*1. The Government*

**31.** The Government accepted that the College was a public body for whose actions the State was directly responsible under the Convention.

**32.** Although there had been some monitoring of the applicant's telephone calls, e-mails and internet usage prior to November 1999, this did not extend to the interception of telephone calls or the analysis of the content of websites visited by her. The monitoring thus amounted to nothing more than the analysis of automatically generated information to determine whether College facilities had been used for personal purposes which, of itself, did not constitute a failure to respect private life or correspondence. ...

**33.** In the event that the analysis of records of telephone, e-mail and internet use was considered to amount to an interference with respect for private life or correspondence, the Government contended that the interference was justified.

**34.** First, it pursued the legitimate aim of protecting the rights and freedoms of others by ensuring that the facilities provided by a publicly funded employer were not abused. Secondly, the interference had a basis in domestic law in that the College, as a statutory body, whose powers enable it to provide further and higher education and to do anything necessary and expedient for those purposes, had the power to take reasonable control of its facilities to ensure that it was able to carry out its statutory functions. It was reasonably foreseeable that the facilities provided by a statutory body out of public funds could not be used excessively for personal purposes and that the College would undertake an analysis of its records to determine if there was any likelihood of personal use which needed to be investigated ...

**35.** Finally, the acts had been necessary in a democratic society and were proportionate as any interference went no further than necessary to establish whether there had been such excessive personal use of facilities as to merit investigation.

*2. The applicant*

**36.** The applicant did not accept that her e-mails were not read and that her telephone calls were not intercepted but contended that, even if the facts were as set out by the Government, it was evident that some monitoring activity took place amounting to an interference with her right to respect for private life and correspondence.

**37.** ... the interference had no basis in domestic ... there was no ... express power for the College to carry out surveillance on its employees and the statutory powers did not make such surveillance reasonably foreseeable.

**38.** The applicant asserted that the conduct of the College was neither necessary nor proportionate. There were reasonable and less intrusive methods that the College could have used such as drafting and publishing a policy dealing with the monitoring of employees' usage of the telephone, internet and e-mail.

**B. The Court's assessment**

**39.** The *Court* notes the Government's acceptance that the College is a public body for whose acts it is responsible for the purposes of the Convention. Thus, it considers that in the present case the question to be analysed under Art. 8 relates to the negative obligation on the State not to interfere with the private life and correspondence of the applicant ...

**40.** The *Court* further observes that the parties disagree as to the nature of this monitoring and the period of time over which it took place. However, the *Court* does not consider it necessary to enter into this dispute as an issue arises under Art. 8 even on the facts as admitted by the Government.

*1. Scope of private life*

**41.** According to the *Court's* case-law, telephone calls from business premises are prima facie covered by the notions of „private life" and "correspondence" for the purposes of Art. 8 § 1 (see *Halford*, § 44 and *Amann v. Switzerland* [GC], no. 27798/95, § 43, ECHR 2000-II). It follows logically that e-mails sent from work should be similarly protected under Art. 8, as should information derived from the monitoring of personal internet usage.

**42.** The applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone (see *Halford*, § 45). The same expectation should apply in relation to the applicant's e-mail and internet usage.

*2. Whether there was any interference with the rights guaranteed under Article 8.*

**43.** The *Court* recalls that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Art. 8 as such information constitutes an „integral element of the communications made by telephone" (see *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, § 84). The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (*ibid*). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Art. 8 § 1 (see *Amann*, cited above, § 65). Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings.

**44.** Accordingly, the *Court* considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Art. 8.

*3. Whether the interference was „in accordance with the law"*

**45.** The *Court* recalls that it is well established in the case-law that the term „in accordance with the law" implies – and this follows from the object and purpose of Art. 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by Art. 8 § 1. This is all the more so in areas such as the monitoring in question, in view of the lack of public scrutiny and the risk of misuse of power (see *Halford*, cited above, § 49).

**46.** This expression not only requires compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law (see, *inter alia*, *Khan v. the United Kingdom*, judgment of 12 May 2000, *Reports of Judgments and Decisions* 2000-V, § 26; *P.G. and J.H. v. the United Kingdom*, cited above, § 44). In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures (see *Halford*, cited above, § 49 and *Malone*, cited above, § 67).

**47.** The *Court* is not convinced by the Government's submission that the College was authorised under its statutory powers to do „anything necessary or expedient" for the purposes of providing higher and further education, and finds the argument unpersuasive. Moreover, the Government do not seek to argue that any provisions existed at the relevant time, either in general domestic law or in the governing instruments of the College, regulating the circumstances in which employers could monitor the use of telephone, e-mail and the internet by employees. Furthermore, it is clear that the Telecommunications (Lawful Business Practice) Regulations 2000 (adopted under the Regulation of Investigatory Powers Act 2000) which make such provision were not in force at the relevant time.

**48.** Accordingly, as there was no domestic law regulating monitoring at the relevant time, the interference in this case was not „in accordance with the law" as required by Art. 8 § 2 of the Convention. The Court would not exclude that the monitoring of an employee's use of a telephone, e-mail or internet at the place of work may be considered „necessary in a democratic society" in certain situations in pursuit of a legitimate aim. However, having regard to its above conclusion, it is not necessary to pronounce on that matter in the instant case.

**49.** There has therefore been a violation of Art. 8 in this regard. ...

*III. APPLICATION OF ARTICLE 41 OF THE CONVENTION*

... **A. Damage**

**53.** The applicant made no claim for pecuniary damage but without quantifying an amount, claimed non-pecuniary loss for stress, anxiety, low mood and inability to sleep. ...

**54.** The Government submitted that ..., as the *Court* had held in a number of cases relating to complaints involving the interception of the communications of suspected criminals by the police, in their view, a finding of a violation should in itself constitute sufficient just satisfaction (see *Taylor-Sabori v. the United Kingdom*, no. 47114/99, § 28, 22 October 2002, *Hewitson v. the United Kingdom*, no. 50015/99, § 25, 27 May 2003 and *Chalkley v. the United Kingdom*, no. 63831/00, § 32, 12 June 2003). Moreover, since the conduct alleged consisted of monitoring and not interception, the nature of such interference was of a significantly lower order of seriousness than the cases mentioned above.

**55.** The *Court* notes the above cases cited by the Government, but recalls also that, in *Halford* (cited above, § 76) which concerned the interception of an employee's private telephone calls by her employer, it awarded GBP 10,000 in respect of non-pecuniary damage. Making an assessment on an equitable basis in the present case, the *Court* awards the applicant € 3.000,– in respect of non-pecuniary damage.

**B. Costs and expenses**

**56.** The applicant claimed legal costs and expenses totalling GBP 9,363 inclusive of value-added tax ...

**57.** ... In the Government's view the sum of GBP 2,000 would adequately cover costs and expenses incurred.

**58.** According to its settled case-law, the *Court* will award costs and expenses in so far as these relate to the violation found and to the extent to which they have been actually and necessarily incurred and are reasonable as to quantum (see, among other authorities, *Schouten and Meldrum v. the Netherlands*, judgment of 9 December 1994, Series A no. 304, pp. 28–29, § 78 and *Lorsé and Others v. the Netherlands*, no. 52750/99, § 103, 4 February 2003). Taking into account all the circumstances, it awards the applicant € 6.000,– for legal costs and expenses, in addition to any VAT that may be payable. ...

*FOR THESE REASONS, THE COURT UNANIMOUSLY*

1. *Holds* that there has been a violation of Art. 8 of the Convention;

2. *Holds* that it is not necessary to examine the case under Art. 13 of the Convention.

3. *Holds*

(a) that the respondent State is to pay the applicant ...

(i) € 3.000,– in respect of non-pecuniary damage;

(ii) € 6.000,– in respect of costs and expenses;

(iii) any tax that may be chargeable on the above amounts;
...

4. *Dismisses* the remainder of the applicant's claim for just satisfaction. ...

**Anmerkung**

**1.** Die Probleme im Zusammenhang mit der Nutzung von Internet und E-Mail am Arbeitsplatz beschäftigen bereits seit einiger Zeit Rspr. (s. z.B. *LAG Hamm* RDV 2005, 170; *BAG* MMR 2006, 94) und juristisches Schrifttum (z.B. *Tinnefeld/Viethen*, NZA 2000, 977 ff.; *Schönfeld/Strese/Flemming*, MMR 2001, 8 ff.; *Ernst*, NZA 2002, 585 ff.; *Weißnicht*, MMR 2003, 448 ff.; *Erler*, Die private Nutzung neuer Medien am Arbeitsplatz, 2003; *Hartig*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 6.2, Rdnr. 78 ff.; *Elschner*, Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2004; *Mengel*, BB 2004, 2014 ff.; *Krauß*, JurPC Web-Dok. 14/2004; *Panzer*, Mitarbeiterkontrolle und neue Medien, 2004; *Schmidl*, MMR 2005, 343 ff.; *Steidle*, Multimedia-Assistenten im Betrieb, 2005; *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 2006).

Mit der vorliegenden Entscheidung erreicht das Thema erstmals auch die Rspr. des *Europäischen Gerichtshofs für Menschenrechte* (*EGMR*). Dieser hatte sich zuvor nur mit der Frage zu beschäftigen gehabt, ob Telefongespräche von Mitarbeitern am Arbeitsplatz „Privatleben" und „Korrespondenz" i.S.v. Art. 8 Abs. 1 EMRK und entsprechend von der Menschenrechtskonvention geschützt sind. Beides wurde in der Vergangenheit bejaht (Halford ./. Vereinigtes Königreich, Slg. 1997-III, Abs. 44; s.a. Kopp ./. Schweiz, Slg. 1998 – II, Abs. 50; Amann ./. Schweiz, Slg. 2000-II, Abs. 44).

**2.** Auf der Schutzbereichsebene überträgt das *Gericht* dies mit wenigen Worten („it follows logically") auf die Nutzung von E-Mail und Internet. Gleichzeitig bestätigt es seine Rspr., wonach auch die Verkehrsdaten (Informationen über den Kommunikationspartner, Zeitpunkt und Länge einer Kommunikation) von Art. 8 Abs. 1 EMRK erfasst sind. Beides entspricht dem Grundrechtsverständnis der deutschen Rspr. zu Art. 10 GG und zum Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und dürfte sachlich unstreitig sein. Da die Bf. von der Überwachung keine Kenntnis hatte, war auch das Kriterium der berechtigten Erwartungen („reasonable expectations") – das dem deutschen Grundrechtsverständnis jedenfalls hinsichtlich des Schutzbereichs fremd ist – erfüllt.

Das *Gericht* verzichtet sodann auf eine genaue Untersuchung der tatsächlichen Überwachungsmaßnahmen und des Ausmaßes der erhobenen und weiterverwendeten Daten. Auf Grund der Tatsache, dass zumindest die Verkehrsdaten aufgezeichnet worden waren, lag auf jeden Fall ein Eingriff vor. Für diesen war mit dem College auch eine Körperschaft öffentlichen Rechts verantwortlich.

Auf der Rechtfertigungsebene konnte sich der *EGMR* auf die Feststellung beschränken, dass zum relevanten Zeitpunkt keine gesetzliche Ermächtigungsgrundlage für die Kontrollmaßnahmen in Kraft war. Nur deswegen war es auch möglich, den genauen Umfang der Überwachung offenzulassen. Wenn nämlich eine Rechtsgrundlage vorhanden gewesen wäre, hätte das *Gericht* den Eingriff i.R.v. Art. 8 Abs. 2 EMRK gegen eines oder mehrere der dort genannten legitimen Ziele abwägen und dabei die Schwere der Beeinträchtigung würdigen müssen. Im vorliegenden Fall musste dagegen weder die Frage beantwortet werden, ob der Eingriff materiellrechtlich zu rechtfertigen gewesen wäre, noch ob die Rechtssetzungsbefugnis angesichts ihrer extremen Unbestimmtheit für so weitgehende Eingriffe wie die TK-Überwachung von Mitarbeitern hinreichend ist (Sec. 19 des Further and Higher Education Act 1992, auf den sich der Bg. stützt, lautet: „A further education corporation may do anything ... which appears to the corporation to be necessary or expedient for the purpose of or in connection with the exercise of any of their principal powers").

Dem Hinweis des *Gerichts*, es erachte den Verweis des Bg. auf das bloße Bestehen einer allgemeinen Satzungsgewalt des Colleges als nicht überzeugend (unpersuasive), kann man nur in aller Deutlichkeit beipflichten. Wenn man das Vorliegen von Kompetenznormen für Grundrechtseingriffe ausreichen lassen würde, gäbe man das Prinzip des Gesetzesvorbehalts auf.

**3.** Im deutschen Recht sperrt bereits § 4 Abs. 1 BDSG einfachgesetzlich jede Form der Datenverwendung, sofern nicht ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da der Fall der Einwilligung zumindest bei größeren Betrieben unrealistisch ist, ist dementsprechend auch für die Überwachung von Beschäftigten ein Erlaubnistatbestand erforderlich. Das können auch Tarifverträge, Betriebs- oder Dienstvereinbarungen sein (*BAG* DB 1986, 2080, 2082; *Walz*, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, § 4

Rdnr. 11). Sind diese nicht vorhanden, bestimmt sich die Zulässigkeit der Überwachung der Telekommunikation in Betrieben und in der Verwaltung auf Grund des Fehlens eines Arbeitnehmerdatenschutzgesetzes nach dem allgemeinen Datenschutz-, TK- und Telemedienrecht.

Dabei ist nach ganz h. A. danach zu differenzieren, ob eine Privatnutzung der TK-Anlagen zulässig ist. Wenn die Privatnutzung gestattet ist, ist der Arbeitgeber oder Dienstherr auch TK-Anbieter (so jedenfalls die ganz h.M., s. nur *Ernst*, NZA 2002, 585, 587; *Steidle*, a.a.O., S. 160 ff.; *Schmidl*, MMR 2005, 343, 344, jew. m.w.Nw.) und muss die entsprechenden Vorgaben des TKG – insb. zum Schutz des Fernmeldegeheimnisses (§ 88 TKG) – erfüllen. Außerdem ist er regelmäßig Diensteanbieter i.S.v. § 2 Nr. 1 TMG. TKG und TMG bieten hier zumindest abgestufte rechtliche Regelungen über die Datenverwendung (ausf. zum Ganzen *Steidle*, a.a.O., S. 249 ff.). Darüber hinaus kann nach der Rspr. unter bestimmten Voraussetzungen § 206 StGB eingreifen (*OLG Karlsruhe* MMR 2005, 178; dazu *Schmidl*, DuD 2005, 267 ff.; *Lejeune*, CR 2005, 290 f.).

Soweit eine private Nutzung von Kommunikationsanlagen ausgeschlossen ist, sind TK- und Telemedienrecht unanwendbar und die Kontrolle wird für Privatunternehmen auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestützt. Im Bereich der Bundesverwaltung verweist § 12 Abs. 4 BDSG ausdrücklich auch hinsichtlich der Erhebung personenbezogener Daten auf § 28 Abs. 1 BDSG. Insoweit gibt es also datenschutzrechtlich keine Unterschiede zwischen den Beschäftigten des öffentlichen Dienstes und in privaten Unternehmen. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die Verwendung zulässig, „wenn es der Zweckbestimmung eines Vertragsverhältnisses ... mit dem Betroffenen dient". Ein Rückgriff auf die Nr. 2 und 3 ist im Arbeitsverhältnis nicht möglich (*BAG* RDV 1987, 129).

**4.** Angesichts dessen könnte man zu dem Ergebnis kommen, dass die vorliegende Entscheidung – da entsprechende Rechtsgrundlagen vorhanden sind – für Deutschland keine oder nur theoretische Bedeutung habe. Dieser Schluss wäre jedoch voreilig, weil das *Gericht* weitergehende Vorgaben aufstellt.

Die Anwendung von § 28 Abs. 1 Satz 1 Nr. 1 BDSG führt nämlich i.E. in schwierige Abwägungsprozesse, für die die Rspr. zwar Kriterien entwickelt hat (s. ausf. *Steidle*, a.a.O., S. 268 ff.; *Simitis*, in: ders., a.a.O., § 28 Rdnr. 45, 101 ff. m.w.Nw.), die jedoch kaum als vom Gesetzgeber vorgegeben betrachtet werden können. Auf dieses Problem soll hier nicht im Einzelnen eingegangen werden. Klar ist jedoch, dass die Formulierung in § 28 Abs. 1 Satz 1 Nr. 1 BDSG („Zweckbestimmung eines Vertragsverhältnisses") überaus unbestimmt ist. Bereits vor dem Hintergrund des deutschen verfassungsrechtlichen Bestimmtheitsgrundsatzes ist dies überaus kritisch zu bewerten.

Diese Kritik wird durch vorliegendes Urteil gestützt, wenn es dort heißt: „In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures". Der *Gerichtshof* stellt damit – wie in früheren Urteilen – nicht nur formale, sondern auch qualitative Anforderungen an die gesetzliche Grundlage (s. zur Rspr. z.B. Rekvényi ./. Ungarn, NVwZ 2000, 421, 422; Vogt ./. Deutschland, NJW 1996, 375, 376; Doerga ./. Niederlande, abrufbar unter: http://www.echr.coe.int/echr, Abs. 50 ff.; *Meyer-Ladewig*, EMRK, 2. Aufl. 2006, Art. 8 Rdnr. 38).

Dies gilt zwar direkt nur für den Bereich der hoheitlichen Datenverwendung (einschl. der hier vorliegenden Verarbeitung von Personaldaten). Der deutsche Gesetzgeber sollte aber die Entscheidung als deutlichen Hinweis darauf verstehen, dass auch auf Grund der völkerrechtlichen Verpflichtungen nach der EMRK eine bereichsspezifische Regelung der Problematik in einem Beschäftigtendatenschutzgesetz erforderlich ist (dazu *Tinnefeld/Viethen*, NZA 2000, 977 ff.; *Simitis*, AuR 2001, 429 ff.; *Steidle*, a.a.O., S. 386 ff.).

*Dr. Gerrit Hornung, LL.M. (European Law), Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel.*