IRIS plus

2011-6

Limits to the Use of Personal Data

LEAD ARTICLE

The Protection of Personal Data and the Media

- Freedom of Information and the Media vs. Personality Rights
- Media and the (Data) Protection of Individuals
- Media and the Protection of User Data

RELATED REPORTING

Balancing Conflicting Interests

- Limits to the Freedom of Information and Expression
- The Right of Reply
- Self-regulation
- Internet Regulation and Freedom of Expression

ZOOM

The Legal Framework for the Use of Personal Data by the Media

- Rights of the Media
- Rights of Data Subjects
- National Regulation

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *plus* 2011-6
Limits to the Use of Personal Data

ISBN (Print Edition): 978-92-871-7291-4
Price: EUR 24,50
European Audiovisual Observatory, Strasbourg 2011

ISBN (PDF-Electronic Edition): 978-92-871-7294-5
Price: EUR 33

IRIS *plus* Publication Series
ISSN (Print Edition): 2078-9440
Price: EUR 95

ISSN (PDF-Electronic Edition): 2079-1062
Price: EUR 125

Director of the Publication:
Wolfgang Closs, Executive Director of the European Audiovisual Observatory
E-mail: wolfgang.closs@coe.int

Editor and Coordinator:
Dr Susanne Nikoltchev, LL.M. (Florence/Italy, Ann Arbor/MI)
Head of the Department for Legal Information
E-mail: susanne.nikoltchev@coe.int

Editorial Assistant:
Michelle Ganter
E-mail: michelle.ganter@coe.int

Marketing:
Markus Booms
E-mail: markus.booms@coe.int

Typesetting:
Pointillés, Hoenheim (France)

Print:
Pointillés, Hoenheim (France)
Conseil de l'Europe, Strasbourg (France)

Cover Layout:
Acom Europe, Paris (France)

Publisher:
European Audiovisual Observatory
76 Allée de la Robertsau
F-67000 Strasbourg
Tel.: +33 (0)3 90 21 60 00
Fax: +33 (0)3 90 21 60 19
E-mail: obs@obs.coe.int
www.obs.coe.int

Contributing Partner Institutions:

Institute of European Media Law (EMR)
Franz-Mai-Straße 6
D-66121 Saarbrücken
Tel.: +49 (0) 681 99 275 11
Fax: +49 (0) 681 99 275 12
E-mail: emr@emr-sb.de
www.emr-sb.de

Institute for Information Law (IViR)
Kloveniersburgwal 48
NL-1012 CX Amsterdam
Tel.: +31 (0) 20 525 34 06
Fax: +31 (0) 20 525 30 33
E-mail: website@ivir.nl
www.ivir.nl

Moscow Media Law and Policy Center
Moscow State University
ul. Mokhovaya, 9 - Room 338
125009 Moscow
Russian Federation
Tel.: +7 495 629 3804
Fax: +7 495 629 3804
www.medialaw.ru

Please quote this publication as:
IRIS *plus* 2011-6, Limits to the Use of Personal Data (Susanne Nikoltchev (Ed.), European Audiovisual Observatory, Strasbourg 2011)

© European Audiovisual Observatory, 2011
Opinions expressed in this publication are personal and do not necessarily represent the views of the Observatory, its members or the Council of Europe.

Limits to the Use of Personal Data

© 2011, European Audiovisual Observatory, Strasbourg (France)

Foreword

At the end of September, Facebook announced a plan to extend their service in order to, as it stated, enable users to create a "Life Archive" and thus offer an unlimited number of "friends" all the details and events of their own lives at the click of a mouse. Who would have thought twenty years ago that this project would on no account be understood as a continuation of Orwell's *1984* but as an offer of a service and business model to be taken seriously? And who would have assumed at that time that, in the light of this and similar services, we would one day be discussing whether and how it would still be possible to exercise control over electronically available personal data? The answer might be that the founding fathers of the European Convention on Human Rights at least considered questions like these to be possible, since there are subjects that lead us to face challenges that date back a long way despite being dressed up in new clothes. In the context of personal data, the answer consists in finding a meaningful balance between the rights to freedom of information and freedom of expression on the one hand and the protection of the personality and the private sphere on the other, and it is these conflicting interests that the Convention has always clearly had in mind.

The idea of a "life archive" consisting of personal data is no doubt an extreme case, but it is a fact that there are numerous occasions in the media field – including the audiovisual media – when the interest of the media in using personal data clashes with the interests of those affected in having their details protected. Here, we only need to think about reports on individuals in public life, news on criminal proceedings or reports by investigative journalism. In the age of bidirectional communication, situations also arise in which the users of media services, too, are concerned about the protection of their own personal data. Media service providers have a considerable interest in producing customer profiles that are as precise as possible, because those who know their customers particularly well can tailor their products and services to them and thus create competitive advantages.

There is no one answer to the question of where the limit to the permissible use of personal data lies because the borderline is ultimately established by weighing up conflicting interests in each individual case. Nonetheless, a number of demarcation lines can be inferred from current case law on limits to freedom of information and freedom of expression imposed on grounds of data protection or privacy protection. However, they are no more than demarcation lines and where they actually run is constantly checked since every new form of data usage and every new situation involving different interests can give rise to new criteria for weighing up those interests. The relevant reflections on the extent of the right to freedom of information

© 2011, European Audiovisual Observatory, Strasbourg (France)

may differ considerably. They may depend on whether, for example, a journalist's interest in conducting research for a television report clashes with the subject's right to privacy or whether a provider of audiovisual media services would now like to use for different purposes the personal information voluntarily supplied by its customer in connection with subscribing to a specific service. By enacting European and domestic law, legislators are trying to create some legal certainty despite the unavoidable uncertainties of a system based in principle on weighing up different interests.

The Lead Article of this IRIS *plus* provides some assistance in unravelling the many possible data usage situations in the overall context of conflicting human rights. It distinguishes between two fundamental situations: firstly, cases in which audiovisual media make data of individuals concerned available and, secondly, cases involving the protection of the data of those who use such media. It explains the existing EU regulations and describes how in various typical situations the interests of the media have been balanced against those of the individuals concerned or of media users.

As the protection of personal data involves fundamental issues relating to the weighing up of human rights, the ZOOM of this IRIS *plus* is devoted to explaining the rights concerned. It describes how the European Court of Human Rights interprets Article 10 of the European Convention on Human Rights ("the Convention"), which is of key importance for audiovisual media services, and how the European Court of Justice has interpreted its equivalent, Article 11 of the EU's Charter of Fundamental Rights (CFR). It then describes how these human rights have been given a more concrete form by secondary legislation. Employing the same dual approach, this question of weighing up interests is discussed with respect to the rights of those affected arising from Article 8 of the Convention and Articles 7 and 8 CFR. The picture is rounded off by taking a brief look at German law, which has been chosen as an example of the various ways of creating domestically relevant provisions.

The Related Reporting section finds its place between the remarks on EU law from the point of view of various scenarios and the discussion of conflicting human rights. It will inform you on developments over the past six months relating to the theme of this IRIS *plus*, i.e. it will discuss the question of determining where to draw the line with regard to using personal data.

Strasbourg, October 2011

Susanne Nikoltchev
IRIS Coordinator
Head of the Department for Legal Information
European Audiovisual Observatory

© 2011, European Audiovisual Observatory, Strasbourg (France)

TABLE OF CONTENTS

LEAD ARTICLE

The Protection of Personal Data and the Media
by Alexander Scheuer and Sebastian Schweda, Institute for European Media Law (EMR), Saarbrücken/Brussels 7

- Freedom of Information and the Media v. Personality Rights 7
- Media and the (Data) Protection of Individuals 9
- Media and the Protection of User Data 21

RELATED REPORTING

Balancing Conflicting Interests
by Dirk Voorhoof(Ghent University (Belgium) & Copenhagen University (Denmark) & Member of the Flemish Regulator for the Media), Sebastian Schweda (Institute of European Media Law (EMR), Saarbrücken/Brussels), Amélie Blocman (Légipresse), Páll Thórhallsson (Legislative Department, Prime Minister´s Office, Iceland and Reykjavik University in Media Law), Damien McCallig (School of Law, National University of Ireland, Galway), Jana Markechova (Markechova Law Offices), Trinidad García Leiva (Universidad Carlos III de Madrid), Manuela Branco (Autorità per le garanzie nelle comunicazioni (AGCOM)), Toby Mendel (Centre for Law and Democracy), Andrei Richter (Faculty of Journalism, Moscow State University) 29

- Limits to the Freedom of Information and Expression 30
- The Right of Reply 36
- Self-regulation 36
- Internet Regulation and Freedom of Expression 42

ZOOM

The Legal Framework for the Use of Personal Data by the Media
by Sebastian Schweda, Institute of European Media Law (EMR), Saarbrücken/Brussels 45

- Rights of the Media 46
- Rights of Data Subjects 49
- National Regulation 52

© 2011, European Audiovisual Observatory, Strasbourg (France)

The Protection of Personal Data and the Media

Alexander Scheuer and Sebastian Schweda,
Institute for European Media Law (EMR), Saarbrücken/Brussels

I. Freedom of Information and the Media versus Personality Rights – an Unresolved Conflict?

"Use public data, protect private data!" This remark, which is ascribed to the hacker and founder of the Chaos Computer Club Wau Holland, encapsulates an important guiding principle of hacker ethics.[1] At the same time, it describes the basic idea behind the European legal rules on media and information freedom on the one hand and data protection on the other. However, what is public and what is private? In the context of forms of information exchange, the so-called Web 2.0 in particular shows that the borderlines between public and private communication are becoming increasingly blurred. The (mass) media, which target the public, are clear evidence that data that may initially have been private can very quickly become public.

The right to freedom of information and to free speech (especially with regard to press and broadcasting freedom) ensures that media can carry out their democratic task of reporting as comprehensively as possible on events of public interest and do so to a large extent without state and private interference.[2] These basic rights enable the media to conduct research to obtain and subsequently publish the information necessary for their reporting. However, there are limits to the exercise of these rights when the rights of other people are affected. If every media user is to be provided with comprehensive information, it is almost always necessary to gather and make available personal (i.e., personally identifiable) data on the subject of the report.

The activities of gathering data (as a manifestation of passive freedom of information) and publishing it (active freedom of information) must always be separated from one another as they are subject to different rules.[3] In the case of both activities, the degree of regulation is guided

1) Cf. http://www.ccc.de/hackerethics
2) See on this ZOOM, section I.
3) See on this Egbert Dommering, "Data, Information and Communication in 21st Century Europe: A Conceptual Framework", in Thomas Kleist/Alexander Rossnagel/Alexander Scheuer (eds.), Europäisches und nationales Medienrecht im Dialog – Festschrift aus Anlass des 20-jährigen Bestehens des Instituts für Europäisches Medienrecht e.V. (EMR), Band 40 der EMR-Schriftenreihe, Baden-Baden 2010, pp. 51 ff., 60. Dommering first draws this distinction between (data) processing and editing: "The first one facilitates the storage of information, the other its communication to the public as a contribution to public debate. So, the former should be subject to the principles of informational privacy, the latter to those of free flow. A press archive accessible to the general public has a supporting role to play in the public debate, but does not in itself form part of that debate. In the context of press law, on the other hand, the fact that there is a greater connection between the archive and the debate needs to be taken into account". He goes on to establish that "the principles of free flow and of informational privacy will need to be specified".

© 2011, European Audiovisual Observatory, Strasbourg (France)

by the adage "A picture says more than a thousand words". If a photographic or even audiovisual documentation is produced showing who met whom and where, then the shooting and publication of a photograph or film constitute the processing of personal data within the meaning of data protection law. When they undertake this processing, the media thus almost inevitably come into conflict with the individual's interest in the protection of his or her personality. This interest is also protected by the provisions of human rights law.

The extent of the personality rights of private individuals comprises on the one hand the protection of privacy, i.e. a private sphere within which information should remain confidential. This sphere is either spatially limited (e.g., the person's own home) or limited in terms of size, as in the case of communications directed at a numerically determinable group. On the other hand, personality rights transcend the purely private sphere and also accord the comprehensive right to be able to control the "image" of oneself made available to others, especially outside the private sphere. This right literally grants the "right to one's own image", that is to say it entitles individuals to decide what photographic images of them are to be made available and to whom. However, individuals also exercise their right to control the use of their images in public when they resist being portrayed in a way that insults their honour or standing. Finally, a "right to informational self-determination" can be inferred from the personality right,[4] which is understood to mean the right to control all information about one's own person, i.e. any item of personal data.[5] The so-called "general personality right" thus not only serves to keep certain information confidential, i.e. in the private sphere. Rather, its purpose is also to safeguard the autonomy and self-determination of individuals, who should be able to decide whether and what information about them may be passed on. In this way, they should determine what pictures of them exist in the public domain.[6]

As early as 1974, the Council of Europe Committee of Ministers called for individuals affected by media reporting to be given the possibility of controlling the way they are portrayed in public. Resolution (74)26[7] accords the individual the right to correct untrue facts and demands that such a correction be made without undue delay and, as far as possible, with the same prominence as in the original publication. Moreover, individuals affected should be able to take action against the publication of facts and opinions[8] that constitute intrusion into their private life or an attack on their dignity, honour or reputation. This right is only restricted if the publication is justified by overriding legitimate public interests or by the (even tacit) consent of the person concerned. Both aspects of the protection of the individual – the right to privacy and the right to the protection of the personality (in the narrower sense described in the previous paragraph of controlling the use of one's own image in public) – can, according to the resolution, therefore be cited against too broad an understanding of freedom of expression. The aforementioned protective measures accordingly contribute – in addition to subsequently developed rules of data protection law to be described below – to striking a balance between the basic rights that conflict with one another.

---

4) The *Bundesverfassungsgericht* (the German Federal Constitutional Court – BVerfG) developed this basic right from the general personality right in the so-called "census judgment" (Collection of Federal Constitutional Court Decisions [BVerfGE] 65, 1, 41 ff., quoted from: http://www.servat.unibe.ch/dfr/bv065001.html).

5) See on the protection of the rights of the individual ZOOM, section II.

6) Andreja Rihter, "Protection of privacy and personal data on the Internet and online media", report for the Committee on Culture, Science and Education of the Council of Europe Parliamentary Assembly, unanimously adopted by the committee on 12 May 2011, available at: http://assembly.coe.int/Documents/WorkingDocs/Doc11/EDOC12695.pdf , p. 8. See also *Thomas Hoeren*, "Persönlichkeitsrechte im Web 2.0", in: Thomas Kleist/Alexander Rossnagel/Alexander Scheuer (eds.), op. cit. (fn. 3), pp. 483 ff., 488: "In such an information society, the personality right has developed into a general right of media and informational self-determination".

7) Committee of Ministers, resolution on the right of reply – position of the individual in relation to the press. The Council of Europe documents are available at https://wcd.coe.int/

8) This goes further than Article 28 of Directive 2010/13/EU (Directive of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive – codified version), OJ EU of 15 April 2010, L 95, pp. 1 ff). The Official Journals of the EU and EC are available at http://eur-lex.europa.eu/

© 2011, European Audiovisual Observatory, Strasbourg (France)

Media mainly gather and use personal data in their external relations since they pass on to the users of their media services data on an individual affected by the media reporting. They also gather and use personal data of these users.[9]

If the person affected (involuntarily) becomes the subject of journalistic activities, the principal aim is to establish the limits to research and the admissibility of reporting that identifies individuals. The first main part of this article (section II) will first of all clarify the rules of European law (data protection and/or media legislation) under which these questions must be assessed. The nature of the protection afforded in individual cases according to the judgments of European and domestic courts will then be pointed out by reference to typified constellations.

In the case of user data protection, on the other hand, classical forms of media use where the consumer's personal data are processed will be discussed, as will new "interactive" media. Although the terrestrial, satellite or, indeed, cable reception of television programmes does not in principle require any data processing, pay-TV services and some additional interactive services (e.g., taking part in lotteries and competitions or voting in "participation TV" shows) can only be offered when the user's personal data are processed.

New challenges for the protection of user data are posed by the media forms that have mainly emerged in the last few years: bidirectional communication paths – especially Internet Protocol based (IP based) – offer their users for the first time a permanent return path. Here, the main aim is the further use of the data for behavioural targeting advertising. Based on the new technical means available, innovative business models have become established on the "Participatory Web" in the form of so-called social networks, such as Facebook, and video portals with "user-generated content" (UGC).

In the second main part of this article (section III) we will first of all describe the technical situation and the possibilities available and then examine the data protection implications of the situations just mentioned. This will be done on the basis of the data protection legislation in force in the EU and the member states of the Council of Europe. Finally, forthcoming developments and their consequences for the relationship between the public and private sphere will be discussed (section IV).

II. Media and the (Data) Protection of Individuals

The constitutional protection of the legal interests of the media, of the subjects of media reporting and of media users is put into concrete form in secondary EU law, which contributes to resolving the conflicting relationship between freedom of expression and personality rights.

Regulation (EC) No. 1049/2001 regarding public access to EU documents[10] protects passive freedom of information. According to Article 1, the widest possible access should be guaranteed

9) However, they also process personal data in internal business processes, for example details of informers and "contributors", such as journalists, editors, presenters, actors, show guests, technicians and other employees of the media company or people commissioned by them, for example when their names are mentioned in the closing credits of a television programme. However, this article excludes these two situations: the protection of informers and editorial confidentiality typically do not involve provisions relating to the conflicting interests of data protection and media freedom. Rather, the concepts behind these terms are characteristics that shape media freedom itself and, with regard to their objective, are supposed to protect the exercise of media activities but only incidentally protect the individuals involved. On the other hand, when it comes to the protection of the personal data of contributors and/or media company employees these protective rights usually do not clash with media freedom. In this case, it must normally be assumed that the person concerned has (effectively) given his or her consent as it is virtually inconceivable that an individual will knowingly and willingly take part in a television film, for example, without agreeing to the publication of his or her actual name or at any rate an identifying pseudonym ("stage name").

10) Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ EC of 31 May 2001, L 145, pp. 43 ff. On the Commission's proposal to adapt the regulation (after the entry into force of the Treaty of Lisbon) and its application in 2010, see the Commission's report of 12 August 2011, COM (2011) 492 final.

© 2011, European Audiovisual Observatory, Strasbourg (France)

and the exercise of the right should be made as easy as possible to ensure the transparency of the work of the EU institutions.[11] The Advocate-General's Opinion in the *Schecke* case makes it clear that a requirement to ensure transparency in public administration is a legitimate ground to limit the right to privacy: the aim to further openness in a democratic society must in principle be applauded but transparency is "not necessarily an absolute good" but "may have to be weighed against another competing objective" in an individual case.[12] As will be shown below, the same applies to the conflict of interests between data protection and freedom of speech or freedom of the media.

Directive 95/46/EC[13] (Data Protection Directive, hereinafter DPD) contains provisions on the protection of personal data. It may not be applied to data processing carried out by "a natural person in the course of a purely personal or household activity" (such as private correspondence) (Article 3, para. 2, second indent). In the *Lindqvist* case,[14] the Advocate-General restricted this limitation of the scope to activities belonging to the private and family lives of individuals, which "obviously" do not include the publication of personal data on the Internet, when the data are made available to an unlimited number of users.[15]

1. Substance and Interpretation of Article 9 DPD

According to Article 9 DPD, member states may provide for exemptions or derogations from data protection rules in the case of data processing "solely for journalistic purposes or the purpose of artistic or literary expression"– but only

> "if they are necessary to reconcile the right to privacy with the rules governing freedom of expression".

Recital 37 of the DPD emphasises that exemptions must be provided for, especially in the audiovisual field. It also states:

> "Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority."

Any derogation must therefore be the result of weighing up the basic rights to freedom of expression and to the protection of the personality. The scope for interpretation granted by Article 9 DPD will probably end where domestic law no longer indicates that those basic rights have been sufficiently weighed up, because the scope of the provision allowing for derogation is either too narrow or too wide.[16]

Since the entry into force of the DPD, the Court of Justice of the European Union (ECJ) has considered the meaning of the rule in two decisions so far.

---

11) For a general discussion of the rights of the media and individuals to information from public bodies, see Thorsten Ader/ Max Schoenthal, Access to Information on Government Action, especially from the Media Point of View, in: European Audiovisual Observatory (publ.), IRIS *plus* 2005-2. (Leading) articles from the IRIS *plus* range are available at http:// www.obs.coe.int/oea_publ/iris/iris_plus/index.html
12) Advocate-General's Opinion of 17 June 2010, Cases C-92/09 and C-93/09, *Schecke*, para. 94. The opinions of the advocates-general and the decisions of the EC/EU courts are available at http://curia.europa.eu/
13) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ EC of 23 November 1995, L 281, p. 31.
14) ECJ, *Lindqvist* judgment of 6 November 2003, Case C-101/01.
15) Advocate-General's Opinion of 19 September 2002 in the *Lindqvist* case, C-101/01
16) Cf. Advocate-General's Opinion of 8 May 2008, C-73/07, *Satamedia*, para. 100, on the "almost entire" exclusion of data protection under Finnish law in the case of data processing for journalism.

© 2011, European Audiovisual Observatory, Strasbourg (France)

The proceedings for a preliminary ruling in the aforementioned *Lindqvist* case concerned the publication of personal data on a website. The accused in the original proceedings, who worked as a catechist in a Swedish parish, had published information about her work colleagues on the parish's web page for parishioners who were preparing for their confirmation. She did not inform her colleagues about this or obtain their consent. In the appeal against the judgment sentencing her to a fine, the domestic court referred the matter to the ECJ, asking it among other things whether the DPD contained unacceptable restrictions on freedom of expression.

The *Satamedia* case[17] concerned a paid service for mobile telephone users that made tax data available by SMS on individuals with a certain minimum income – data made publicly available by the Finnish tax authorities. After the Finnish Data Protection Ombudsman had initially unsuccessfully called for the text-messaging service to be closed down, the matter was brought before the Finnish Supreme Administrative Court, which, inter alia, asked the ECJ whether the activities of the two companies involved could be regarded as data processing solely for journalistic purposes.

a) Does the case involve data processing within the meaning of the Directive?

In both cases, the question of whether the use of the content involved was data processing at all within the meaning of the DPD became relevant. It should be noted that in the Advocate-General's Opinion issued in the *Satamedia* case in 2008 and endorsed by the Court, gathering and publishing data in printed form, transferring data onto a CD-ROM, processing data for a database and making data available by SMS service were described as processing personal data without any discussion of the different processes involved, whereas in its 2003 judgment in the *Lindqvist* case the Court discussed in detail whether uploading data to a website (in the form of a transmission to a third country) in itself constituted data processing. Although the ECJ referred in general terms to the state of development of the Internet at the time when the Directive was drawn up and to the fact that the Directive contains no specific criteria for the use of the Internet, it accepted that it constituted data processing without conducting a lengthy discussion at that time. Making information available at a website "entails ... the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet".[18]

b) What must be regarded as journalistic (artistic, literary) activity?

In the ECJ's view, when it comes to classifying an activity as being solely for journalistic purposes the actual medium used to convey the information is unimportant. Accordingly, whether the data are printed on paper, transmitted by radio or transported electronically, such as via the Internet, "is not determinative". This means that Internet blogs, too, should in principle not be exempted from the application of Article 9 DPD.

The Court defines in functional terms when data processing is for *journalistic* purposes pursuant to Article 9 DPD: not only media companies could claim they were engaged in such processing but also anyone working as a journalist.[19] The Advocate-General explained this as follows:

> "At one time journalism was confined to media which were (relatively) clearly recognisable as such, namely the press, radio and television. Modern means of communication such as the internet and mobile telecommunications services are used just as much for the communication of information on matters of public interest as for purely private purposes. Consequently, although the type of communication is an important factor in determining whether journalistic purposes are being pursued, the subject-matter should not be disregarded either."

---

17) ECJ, *Satamedia* judgment of 16 December 2008, C-73/07.
18) ECJ, *Lindqvist* case, op. cit., para. 26.
19) ECJ, *Satamedia* judgment of 16 December 2008, C-73/07, para. 59. See also European Court of Human Rights, *Társaság a Szabadságjogokért (TASZ) v. Hungary* judgment of 14 April 2009, Application No. 37374/05, in which the Court acknowledges that an interest group can act as a "public watchdog" by providing information. The judgments of the European Court of Human Rights are available at: http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en

© 2011, European Audiovisual Observatory, Strasbourg (France)

However, when is the substantive criterion "solely for *journalistic* purposes" met? The ECJ understands this to refer to activities whose object is "the disclosure to the public of information, opinions or ideas".[20] On the one hand, it emphasised "the importance of the right to freedom of expression in every democratic society" and the need to give a broad interpretation to terms relating to that freedom, including journalism. On the other hand, in order to strike a balance with the basic right to the protection of privacy, exemptions and derogations with regard to data protection should remain limited to what is absolutely necessary. In this connection, the ECJ also noted that the Advocate-General had pointed to the need not to take together the concepts of journalistic, literary or artistic purposes and equate them with freedom of expression as they would otherwise (no longer) have any function of their own.[21]

"To give further definition to the concept of journalistic purposes", the Advocate-General had stressed the role of a free press as a "public watchdog" and inferred from this a "duty to impart information and ideas on all matters of public interest". The question, she said, was not whether data was commented on by editors, and the mere fact of making raw data available could contribute to public debate. The Advocate-General thus differs in her understanding of the concept from the German provisions implementing Article 9 DPD, which refer to data processing "exclusively for [the media's] own journalistic-*editorial* … purposes".[22] According to the Advocate-General, there can be assumed to be a public interest when the information and ideas

> "link up with a public debate which is actually taking place or where they concern questions which, according to domestic law and social values, are by nature public issues".

The latter group include public court proceedings, the transparency of political life and the conduct of prominent politicians. On the other hand, the Advocate-General points out, there is no public interest when details of an individual's private life with no connection with a public function are involved, "particularly where there is a legitimate expectation of respect for private life". However, it is at least partly up to the media to create public interest in the first place. Predicting whether this could succeed should not be left up to the state as that would risk setting out on the path of censorship. Accordingly, only in obvious cases should state bodies assume there is no public interest.

The ECJ has so far not discussed in detail in its judgments when it may be assumed that personal data are processed for *artistic* or *literary* purposes. In the *Lindqvist* case, the Commission did classify Internet pages like the one in issue as "an artistic and literary creation" within the meaning of Article 9 (of Directive 95/46)",[23] but the ECJ did not go into this argument in any detail in its judgment. A precise legal classification, especially of borderline cases (for example, documentary films or infotainment formats) has therefore yet to be provided. However, if an item is at least more than the mere expression of an opinion as it constitutes a "journalistic", "artistic" or "literary" media offering, then any further narrowing down to the actual alternative is unnecessary since the legal consequence is the same.

---

20) ECJ, *Satamedia* case, op. cit., para. 61. However, it should be pointed out that according to Recital 47 the mere conveyor of content is not normally regarded as responsible for the data processing within the meaning of Article 2(d) DPD (see on this ZOOM, section II. 2. a). Rather, the person responsible for the data processing is usually "the person from whom the message originates". According to Article 9 DPD, only that person could therefore claim an exemption in respect of certain content under the conditions set out here.

21) Unless otherwise indicated, the following remarks originate from the Advocate-General's Opinion in the *Satamedia* case, paras. 56 ff., 66 f., 73, 77f., 80f., 85.

22) Cf. section 41(1) of the *Bundesdatenschutzgesetz* (Federal Data Protection Act – BDSG). However, the *Bundesgerichtshof* (Federal Court of Justice – BGH) assumed that this precondition already exists when the publication is targeted at an indeterminate group of people and the intention is to express an opinion. See Sebastian Schweda, IRIS 2011-5/12, and Anne Yliniva-Hoffmann, IRIS 2010-2/9. All IRIS Newsletter contributions are available at http://merlin.obs.coe.int . Therefore, under German law, too, the determining factor with regard to who may claim the so-called "media privilege" is not the form of the publication but only the activity itself – which must be journalistic in nature. Internet portals can thus also claim this protection.

23) ECJ, *Lindqvist* case, op. cit., para. 33.

© 2011, European Audiovisual Observatory, Strasbourg (France)

c) When is the processing of data solely for the purposes mentioned?

The requirement that the data processing be *solely for journalistic purposes* does not mean that it must involve "the direct communication of such information" since prior research necessary for a publication is also covered by this provision. In the Advocate-General's view, a decision on whether data processing in an individual case is *solely* for journalistic purposes "requires an appraisal of the objective in question" concerned, and the purpose must be based on objective factors. Subjective aims of the person responsible for the data processing are, she says, accordingly not relevant.

According to the ECJ, the intention to make a profit does not preclude the publication of data being considered as being "solely for journalistic purposes". Rather, "a degree of commercial success may even be essential to professional journalistic activity".[24]

d) Other examples of cases tried in member states

The question of whether personal data may be processed for journalistic purposes may also be relevant in the context of online rating platforms. For example, if an actor's performance is rated in a film critique on an online review page, personal data are inevitably published at the same time. In two domestic judgments concerning the legality of an Internet platform for rating the professional proficiency of teachers (spickmich.de and note2be.com), the German *Bundesgerichtshof*[25] *and the Paris Tribunal de Grande Instance* (TGI)[26] reached different conclusions: although broadly comparable, the business model of spickmich.de was held to be lawful, whereas that of note2be.com was not.

Both courts first considered the relationship of freedom of expression with the right to informational self-determination (as part of the teacher's personality right). In the BGH's view, storing the data did not conflict with the plaintiff's legitimate interests because the assessments complained about only concerned her professional work. It emphasised that participation in an opinion forum must always be permissible when personal data are provided since freedom of expression and freedom of information would otherwise "be limited to statements without any content protected under data protection legislation". The court went on to say that the consent of the person concerned could not be expected in the case of adverse criticism, so that any assessments would thus be "largely rendered impossible". In the Federal Court's opinion, the German provision implementing Article 9 DPD was not relevant in that case as the requirement that processing be "exclusively for their own journalistic-editorial purposes" could only be said to have been met "when the opinion-forming effect for the general public is a defining element of the offering and does not merely play a subsidiary role". The platform operator's offering, the court said, had not met that condition.[27]

The TGI did not even discuss Article 9 DPD. Instead, it weighed freedom of expression and freedom of information against the integrity of the education system. As the court was of the opinion that the publication of teacher ratings mentioning names was likely to have an adverse impact on that integrity, it issued an injunction.

---

24) ECJ, *Satamedia* case, op. cit., para. 82. According to what has been said previously, it may only no longer be possible to assume that solely journalistic purposes are being pursued when the commercial interests relate to a publication that does not serve to disseminate information or ideas on matters of public interest (e.g., regular advertisements in newspapers, cf. Advocate-General's Opinion, para. 84).

25) BGH, judgment of 23 June 2009, Ref. VI ZR 196/08, available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=2f87ec5b9cc2c0d5e8fe748b700898ea&nr=48601&pos=0&anz=1

26) TGI, injunction of 3 March 2008, No. RG 08/51650, available at http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/tgi-par20080303.pdf . The injunction was confirmed by order of the *Cour d'appel de Paris* (Paris Court of Appeal) of 25 June 2008, No. RG: 08/04727, available at http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/ca-par20080625.pdf

27) BGH, op. cit (fn. 25), para. 21. In principle, however, the BGH regards the "electronic press" as covered by the protection of press freedom; cf. BGH, op. cit (fn. 25), para. 20.

© 2011, European Audiovisual Observatory, Strasbourg (France)

e) Future development of the exemption clause

In its proposals to reform EU data protection law[28] the Commission did not comment on the rule contained in Article 9 DPD. However, in its statement the European Parliament[29] pointed to the importance of the provision and called on the Commission in this connection to make every effort "to evaluate the need for developing these exceptions further ... in order to protect freedom of the press". Against the background of technological developments, the Parliament wants to ensure that a high level of data protection is maintained and at the same time that "a fair balance between the right to protection of personal data and the right to freedom of speech and information" is guaranteed.

The European Data Protection Supervisor (EDPS) recognises the cultural differences between the member states with regard to freedom of expression and recommends that, with the exception of modernisation in the light of current Internet developments, the area governed by Article 9 DPD should be excluded from any further efforts at harmonisation.[30] The European Broadcasting Union (EBU) comes out even more clearly in favour of retaining[31] and strengthening the exemption provision. With regard to the Commission's proposal to create a "right to be forgotten", the EBU urges caution: the individual's right to have control over his or her private information must, it says, be separated from the "capacity to disappear from the public record", going on to say that "(t)he media's role in providing that public record needs to be protected for the benefit of society as a whole".[32]

2. Balancing the Interests of the Media Against those of the Individuals Concerned

The conflicting interests of media freedom and the protection of the personality mainly concern two situations (see section I): on the one hand, the question of the legality of the processing of personal data prior to their potential publication, that is to say in connection with research following which a decision is taken on whether and, if so, to what extent the material for a report is suitable and should be used; and, on the other hand, the moment when the information is actually made available to the public. Reports on criminal proceedings where there is a public interest in obtaining information, on the private and intimate lives of individuals in the public eye (politicians, celebrities) and on situations on which information has been unlawfully obtained can seriously affect the rights of the people concerned.

a) "Editorial data protection" – Gathering and use of personal data "within the editorial office"

In order to strike a proper balance, individual protective rights must be framed in such a way that they allow the media sufficient scope for their research. The media must at least have the right to research all the personal data that they might subsequently publish.

---

28) COM, Communication of 4 November 2010 to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final.
29) European Parliament, resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union, P7_TA(2011)0323, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//EN
30) EDPS, Opinion on the Communication from the Commission – "A comprehensive approach on personal data protection in the European Union", OJ EU of 22 June 2011, C 181, pp. 1 ff.
31) Likewise the German television channel Zweites Deutsches Fernsehen (ZDF), which referred in particular to the Federal Court of Justice's broad interpretation of the exemption in the *Satamedia* case (op. cit.); http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/zdf_de.pdf
32) EBU, Comments concerning the consultation on the Commission's Communication – "A comprehensive approach on personal data protection in the European Union", 14 January 2011, available at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/ebu_en.pdf

© 2011, European Audiovisual Observatory, Strasbourg (France)

Journalists are therefore always granted a broad right to conduct research and will even have to have an extensive research obligation imposed on them to guarantee balanced reporting. Precautionary claims for injunctive relief filed by people affected would thwart such research. For example, when hidden cameras are used to reveal potentially illegal or reprehensible activities by the individual concerned, the basic facts must first be established to assess whether it is worthwhile reporting on the case. At least when it is conceivable that the information may be lawfully used, precautionary legal protection against research activities must accordingly not be granted.[33] Only when it becomes clear from the nature of the research that the reporting will be unlawful and the person concerned will consequently be caused irreparable harm can it be prohibited.[34] There are also important limits to research in the context of court proceedings, especially video recordings of trials.[35]

Conversely to what has been said above, the principle must also apply that data that could not be lawfully obtained may only be published in exceptional cases despite freedom of expression. The fact that the person concerned has not broken the law may prove to be an important distinguishing criterion here.[36]

b) Striking a balance between media freedom and the protection of the personality in connection with the publication – reporting that identifies individuals

aa) News reporting on official and judicial proceedings, especially criminal trials

The European Court of Human Rights recognises the right of the media to report on criminal proceedings to inform the public[37] and refers in this connection to Committee of Ministers Recommendation Rec(2003)13.[38] However, it emphasises at the same time that sight must not be lost of the standard of journalistic care, pointing out that "(t)he exercise of freedom of expression carries with it duties and responsibilities, which also apply to the press".[39] In particular, statements that adversely affect the chances of the person concerned to receive a fair trial in accordance with Article 6 para. 1 of the European Convention on Human Rights may be unlawful.[40]

In connection with photo reporting, the "protection of the reputation or the rights of others" may in particular justify interference with freedom of expression.[41] In the *Österreichischer Rundfunk* case,[42] the European Court of Human Rights criticised a court injunction against the Austrian public service broadcaster ORF as being incompatible with the right to freedom of expression (Article 10 of the Convention). The injunction prohibited ORF from showing the picture of a convicted neo-Nazi in connection with a report on his conviction if he had already served his sentence or had been released on parole. The European Court of Human Rights assessed the lawfulness of the restriction on freedom of expression solely by weighing up the following criteria: "the degree of notoriety of the person concerned, the lapse of time since the conviction and the release, the nature of

33) Cf. *Oberlandesgericht Düsseldorf* (Düsseldorf Court of Appeal), judgment of 8 March 2010, Case 20 U 188/09 concerning the secret making of video recordings in a doctor's surgery, available at http://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2010/I_20_U_188_09urteil20100308.html. The court held that it was possible for video reporting to be lawful if the person shown could not be identified. On the situation under French law, see Amélie Blocman, "Hidden Cameras", IRIS 2009-10/12.

34) This was argued by the *Oberlandesgericht Koblenz* (Koblenz Court of Appeal) in its decision of 27 May 2010, Case 4 W 170/10. The case involved a doctor investigated after a number of his patients had died. After the investigations had been discontinued, interviews with two of his patents were planned as part of a television report. The doctor obtained an injunction against his being named in this context.

35) See on this also ECHR, *B. and P. V. United Kingdom* judgment of 24 April 2001, Applications Nos. 36337/97 and 35974/97.

36) See on this question the judgment of the German Federal Constitutional Court described below (section II. 2. c).

37) ECHR, *Dupuis and others v. France* judgment of 7 June 2007, Application No. 1914/02, para. 42.

38) Recommendation of 10 July 2003 of the Committee of Ministers to member states on the provision of information through the media in relation to criminal proceedings. See on this ZOOM, section I. 2.

39) ECHR, *Eerikäinen and Others v. Finland* judgment of 10 February 2009, Application No. 3514/02, para. 60; *Flinkkilä and Others v. Finland* judgment of 6 April 2010, Application No. 25576/04, para. 77.

40) ECHR, *Worm v. Austria* judgment of 29 August 1997, Application No. 83/1996/702/894.

41) ECHR, *Egeland and Hanseid v. Norway* judgment of 16 April 2009, Application No. 34438/04, para. 59.

42) ECHR, *Österreichischer Rundfunk v. Austria* judgment of 7 March 2007, Application No. 35841/02.

© 2011, European Audiovisual Observatory, Strasbourg (France)

the crime, the connection between the contents of the report and the picture shown and the completeness and correctness of the accompanying text". The Court stressed the differences from another case involving the same parties[43] that it had dismissed as inadmissible. In connection with a report on a series of letter bombs, ORF had shown the picture of a former suspect but neither mentioned the acquittal of the person depicted nor the fact that he had already served his sentence for another offence. At that time, the Court did not regard the injunction issued by the domestic court as a violation of Article 10 of the Convention.

The media often report on sensational crimes as early as the hunt for the perpetrator. In most cases, the obligations to be observed in the case of press and radio/TV reporting or, reporting in other audiovisual media do not differ from one another, so a number of judgments on press reporting will be described below.

In the *A. v. Norway* case, for example, the European Court of Human Rights ruled that reports prejudging the applicant constituted a violation of Article 8 of the Convention. The applicant had been questioned as a witness as part of police investigations to solve a crime against two children. The subsequent reporting in a newspaper was such that it suggested he was suspected of committing the offence. Although his name was not mentioned, acquaintances were able to identify him from the photographs published in the media and the details of his place of residence and workplace. The Court established that the publications constituted a particularly serious instance of prejudging of the applicant that was "harmful to his moral and psychological integrity and to his private life".

A case involving the Spanish newspaper *El Mundo*, which had reported on the suspected transactions of illicit funds by the wife of a court president, concerned the extent of a journalist's duty of care.[44] The European Court of Human Rights did not believe there had been a violation of Article 8 of the Convention, stating that the newspaper had exercised the necessary care when carrying out the research as it had adequately checked the sources: the truth of the data on a diskette supplied anonymously had been confirmed in an interview by the then company accountant. Moreover, the report had contained the company's different account of the facts.

In this connection, it should be noted that some personal data are subject to special protection under the law: for example, a duty of confidentiality – for the protection of a particular confidential relationship and/or owing to overriding public interests – arising from the relationship protected by Articles 6 (right to a fair trial) and 8 of the Convention between lawyer and client[45] (as well as between doctor and patient, pastor and individual in need of help, etc). Repeated judicial disputes take place about whether it is permitted to report on relevant cases by quoting (parts of) letters from lawyers. The very publication of the fact that a lawyer-client relationship exists affects the interests of the lawyer and his or her client who is seeking justice. Nonetheless, the highest German courts have ruled that it is generally not permissible to publish such quotations.[46] As far as we can tell, however, the decisions concerned "only" dealt with the lawyer's personality rights and right to exercise his or her profession. It has so far not been clarified whether the client's interest in personal data protection can outweigh the media interests protected by freedom of expression and freedom of the media.

These cases illustrate the duties of care to be observed by the media when reporting on judicial or administrative proceedings. However, according to the established case law of the European Court of Human Rights the state itself is also obliged not only to respect an individual's personality rights but also actively to protect them and must accordingly take appropriate action in its sphere of influence to counter potential violations by the media. "Reality TV" formats that involve media

43) ECHR, *Österreichischer Rundfunk v. Austria* judgment of 25 May 2004, Application No. 57597/00.
44) ECHR, *Polanco Torres and Movilla Polanco v. Spain* judgment of 21 September 2010, Application No. 34147/06.
45) See on this Dean Spielmann, "Das anwaltliche Berufsgeheimnis in der Rechtsprechung des EGMR", *Österreichisches Anwaltsblatt*. 2010, 34 ff., available at http://www.rechtsanwaelte.at/pdfsuche/10_anwbl0708.pdf ; and ECJ, judgment of 14 September 2010 , C-550/07, *Akzo*, paras. 40 ff., 92 ff.
46) Cf. Federal Constitutional Court, decision of 18 February 2010, Ref. 1 BvR 2477/08, http://www.bverfg.de/entscheidungen/rk20100218_1bvr247708.html

© 2011, European Audiovisual Observatory, Strasbourg (France)

representatives accompanying public authority staff in the field are problematic in this connection. Examples of this are video reporting on the execution of a judgment in the home of a debtor, reports on police traffic checks and criminal investigations and on the activities of the social services or employment exchanges.[47] The resulting "exposure" of individuals shows the lack of an appropriate balance from the point of view of data protection law between the public's right to information and the personality rights of the person concerned.[48] However, this type of reporting is particularly questionable because the authorities involved do not seem to provide a sufficient guarantee of protection for that person, who is caught unawares at his or her front door or taken aback by the unexpected encounter with the authorities. The state could comply with its positive duty to provide protection if its employees at least informed the person concerned about his or her rights, and especially about the voluntary nature of co-operating on the reporting of the case, before the journalists begin their work.[49]

In the case of Web 2.0, it is possible to express one's own opinion, for example in vlogs or podcasts, without meeting any particular technical, financial or personal conditions, but private individuals who make use of their freedom of expression may have to comply with certain duties of care. However, the standard is way below that applicable to representatives of the media, as the German Federal Constitutional Court decided in the following case: a committee member of a private club had accused an internationally operating German chemical company in a leaflet of supporting and financing "right-wing compliant" politicians, citing several identical media reports. The Court acknowledged that the press had "a special duty of care in the dissemination of negative facts" but said that in the case of private individuals that duty only applied to facts arising from "their own area of experience and control". It went on to say that, especially in the case of events of public interest in "non-transparent areas of politics and the economy", people depended on media reporting since their own research normally could not turn up sufficient evidence. If that were to be demanded, it pointed out, the result would be to paralyse individual freedom of expression.[50]

In the *Thorgeirson*[51] *and Marônek*[52] cases, the European Court of Human Rights examined a violation of the freedom of expression of the writers of open letters printed in newspapers. In each case, the authors had been convicted at first instance for defamation. A possible violation of press freedom had not been alleged and had therefore not been explicitly examined. However, the European Court of Human Rights evidently assumed that the mere publication of the open letters by an organ of the press did not in itself afford the authors the protection of press freedom. Conversely, the special duty applying to professional media to respect the personality rights of others probably does not apply to those who only occasionally make use of freedom of expression – including, and especially, via the new offerings of the "Participatory Web".

---

47) In connection with (suspected or actual) criminal offences committed by celebrities, there have also been an increasing number of examples in the past of state prosecuting authorities contributing to media reporting that interferes to a significant extent with the personality rights of the individuals concerned. This includes the presentation of the arrested Dominique Strauss-Kahn, then head of the International Monetary Fund (on the lawfulness of this so-called "perp walk" under US law, see http://www.sueddeutsche.de/kultur/perp-walk-von-strauss-kahn-handschellen-zieren-jeden-verdacht-1.1098660). It also includes the leaking of details from the investigation file against the well-known meteorologist and television presenter Jörg Kachelmann (who obtained an injunction against the media; see http://www.dr-bahr.com/news/presserecht/verbreitung-von-kachelmann-fotos-bei-hofgang-in-jva-rechtswidrig.html) and the arrest and indictment of a German girl group singer for grievous bodily harm and the public statement that she had had unprotected sexual intercourse despite being aware of her HIV infection. See on this Gernot Lehr, "Es darf nicht vorverurteilend berichtet warden" – Interview, *epd medien* 2011 (Issue 23), pp. 3 ff.

48) This was criticised by the Conference of the Data Protection Commissioners of the Federation and the *Länder* on support for the judicial authorities for Reality TV programmes in its resolution of 24 June 2010. See "Die Landesbeauftragte für Datenschutz und Informationsfreiheit im Saarland, 23. Tätigkeitsbericht", Saarbrücken 2011, p. 123 f., available at http://www.landtag-saar.de/dms14/So14_0425.pdf

49) Cf. Robert Rittler, "Austria: TV Reporting Consent Considered Given Unless Opposition Expressed", IRIS 2010-1/8.

50) BVerfGE 85, 1, 22; para. 62 (quoted from http://www.servat.unibe.ch/dfr/bv085001.html#Rn062).

51) ECHR, *Thorgeir Thorgeirson v. Iceland* judgment of 25 June 1992, Application No. 13778/88.

52) ECHR, *Marônek v. Slovakia* judgment of 19 July 2001, Application No. 32686/96.

© 2011, European Audiovisual Observatory, Strasbourg (France)

bb) Access to reporting via archives and search engines

Even if reporting that identifies individuals through administrative or judicial proceedings is permitted, in view of current case law the question arises as to what period of time such reports may be kept available in extensive news archives on the Internet, for example. The cases decided up to now have mostly related to online press archives. With the emergence of media libraries, which, at least for a specific period, offer content on the Internet previously transmitted on linear television, the same problem arises in the case of audiovisual content.

In this connection, in Germany the BGH has recently had an opportunity on several occasions[53] to consider the fundamental issue of weighing up conflicting interests. The murderer of an actor released on parole in January 2008 brought an action against the publication at an Internet news portal of an article dated 12 April 2005 reporting that a court was examining whether to re-open the proceedings and mentioning his full name. However, the BGH reached the conclusion that the public interest in being informed and the defendant's right to freedom of expression outweighed the perpetrator's interest in rehabilitation. With the passing of time, the court said, the latter gained in importance when weighing up the conflicting interests but the detrimental effect caused by mentioning the individual's name was insignificant. It went on to say that the case involved a pertinent and objective account of truthful statements and the article had been filed as an "old news item" in the archive section of the portal and could only be located by running a targeted search. A general obligation to remove all articles identifying the perpetrator would unacceptably restrict freedom of expression and the media.

The ECJ will soon rule on the responsibility of search engines for the results they display (which may be both still pictures and videos). In response to a request by various individuals, the Spanish data protection authority (*Agencia Española de Protección de Datos* – AEPD) demanded that Google remove from search results links to online articles already published a long time back in order to guarantee the protection of personal data. A particularly instructive case concerned an article published in 1991 in the Spanish daily newspaper *El País* concerning an action brought against a plastic surgeon for an alleged instance of medical malpractice. The search results listed the subsequent, very short article on the exoneration of the surgeon from the allegations in a much less prominent position than the actual article. The AEPD ruled in its decision of 4 February 2009[54] that the article itself did not have to be removed, pointing out that the Spanish Constitutional Court had made it clear that freedom of information, enshrined in the country's constitution, took precedence over the right to privacy if the facts communicated were true and of public importance. Unlike the single article, however, the Google search compilation and subsequent search results did not fall within the scope of freedom of information. Google appealed against this decision to the *Audiencia Nacional*, which referred the case to the ECJ.[55] Google is worried that the "right to be forgotten" currently being discussed could turn out to be a way of censoring unwelcome material and shift the balance between the protection of personality rights and freedom of expression, the press and information, to the detriment of the latter.

cc) Reporting on (other) prominent individuals

In its decision in the *Caroline von Hannover* case, the European Court of Human Rights considered the publication of photographs from the princess's private life with reference to Article 8 of the Convention. It confirmed that the publication of photographs showing the applicant going about her

53) Op. cit. (fn. 22). See, however, ECHR, judgment of 10 March 2009, *Times Newspapers v. the United Kingdom*, 3002/03 and 23676/03, in which the Court denied that there had been a violation of Article 10 para. 1 of the Convention because the demand that a notice drawing attention to court proceedings on the case be attached to the allegedly libellous articles in the online archive did not disproportionately restrict freedom of expression – after all, no demand had been made that the articles be completely removed from the internet archive.

54) AEPD, Resolution of 4 February 2009, No. R/00155/2009, available at http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01335-2008_Resolucion-de-fecha-04-02-2009_Art-ii-culo-17-LOPD_Recurrida.pdf

55) See Josh Halliday, "Europe's highest court to rule on Google privacy battle in Spain", 1 March 2011, http://www.guardian.co.uk/technology/2011/mar/01/google-spain-privacy-court-case

© 2011, European Audiovisual Observatory, Strasbourg (France)

daily life was protected by the right to freedom of expression but emphasised that the publication interfered with her privacy. The crucial factor when weighing up both basic rights was, the Court said, whether the photograph contributed to a public debate on a matter of general interest.[56] That, in its opinion, was not the case where private pictures of a "public figure" with no official political function were concerned. The public had no legitimate interest in knowing where the applicant was and how she generally behaved in her private life. Any public interest existing nonetheless had to "yield to the applicant's right to the effective protection of her private life".

However, the European Court of Human Rights ruled in *Max Mosley v. the United Kingdom* that Article 8 of the Convention did not demand that the person concerned be notified in advance about a report planned on him or her. In the case in issue, the British weekly newspaper *News of the World* had had video recordings made of the sex life of Max Mosley, the former President of the *Fédération Internationale de l'Automobile*, showing him with prostitutes. The images were published on the Internet by the newspaper together with an article on the applicant's sexual activities. Mosley filed an application with the European Court of Human Rights for a breach of his privacy, which could only have been prevented by an injunction under British law. The Court noted that, as no rule of British law provided for the person concerned to be notified in advance, he had been unaware of what was happening and been unable to apply for an injunction, and that this violated Article 8 of the Convention. The Court acknowledged that the protection of the rights of others in the audiovisual media was particularly important because the latter often had a more direct and more powerful effect than the print media and said it could not see "any possible additional contribution" to a debate of general public interest. It seemed that the material had only been recorded to satisfy public curiosity and shame the applicant. However, the Court held that Article 8 did not call for a statutory obligation to notify the person concerned in advance. Weighing up the conflicting interests had to take account of the limited scope for restricting freedom of the press under Article 10 of the Convention. In general terms, the Court saw the danger of the "chilling effect which would be felt in the spheres of political reporting and investigative journalism, both of which attract a high level of protection under the Convention" and pointed out that this "might operate as a form of censorship prior to publication". It accordingly ruled there had been no violation of Article 8 of the Convention.[57]

Under Polish law, there is an obligation to obtain prior consent in the case of interviews recorded in sound or vision, and this obligation proved problematic in the following case: the chief editor of a newspaper was convicted of publishing extracts of an interview with a politician, who had agreed to the interview but refused to give the prior consent required by law to an edited and considerably shortened version. The European Court of Human Rights regarded the editor's conviction for a breach of the obligation to obtain consent as a violation of Article 10 of the Convention as it could have a deterrent and disproportionate effect on the press. The Court took account in its assessment of the voluntary nature of the interview and the fact that the Polish Press Act provides for a punishment irrespective of the content of the statements made but said that that could not be reconciled with the case law principles relating to Article 10, according to which "the limits of acceptable criticism are wider as regards a politician as such than as regards a private individual". The obligation to obtain consent meant politicians were given "carte blanche" to prevent their own embarrassing statements from being published. Moreover, Polish law provided other remedies for subsequent protection against breaches of privacy. The Court considered it simply paradoxical that the Press Act permitted the publication without prior consent of paraphrased interviews and interviews simply taken down in writing while the statements actually made were subject to prior approval.[58]

In the United Kingdom, the practice of so-called "super-injunctions" has only recently been the focus of public interest.[59] This type of judicial order not only prohibits reporting on a particular situation in a form that identifies the person concerned (compare this with the "simple" injunction that came to the fore in the *Mosley* case) but also on the fact that such an injunction has been

56) ECHR, *Hannover v. Germany* judgment of 24 June 2004, Application No. 59320/00, paras. 52, 59f., 76.
57) ECHR, *Mosley v. the United Kingdom* judgment of 10 May 2011, Application No. 48009/08.
58) ECHR, *Wizerkaniuk v. Poland* judgment of 5 July 2011, Application No. 18990/05.
59) Master of the Rolls, Report of the Committee on Super-Injunctions of 20 May 2011, available at http://www.judiciary.gov.uk/Resources/JCO/Documents/Reports/super-injunction-report-20052011.pdf

© 2011, European Audiovisual Observatory, Strasbourg (France)

issued. A super-injunction thus normally only becomes public knowledge when it is lifted or debated in parliament (which is legally permissible under parliamentary privilege). A breach of such an injunction is punishable by up to two years' imprisonment. In 2011, the case of a married British footballer who had allegedly had an affair with a Welsh model attracted particular attention. Concerned that his former lover might release the details to the media, he met her twice in different hotels but refused to give her the money she had allegedly demanded. Press photographers were evidently informed about the meeting and photographed the sportsman on the way to the hotels. He obtained a super-injunction to ensure that his name would not be mentioned in connection with the affair but a journalist operating anonymously breached the order and published an item via the short news service *Twitter* naming the footballer in connection with the alleged affair.

An even more restrictive form of a "gagging order" became known in March 2011:[60] the so-called "hyper-injunction" even prohibits the person at whom it is directed from informing a member of parliament about the subject of the injunction concerned.

c) Publication of unlawfully obtained information

The subjects on which media can report may depend on how the information has been obtained. In the *Fressoz and Roire* case, the European Court of Human Rights considered whether the publication of confidential national tax authority documents on the income of the former chairman and managing director of Peugeot S.A. was justified under Article 10 of the Convention.[61] The applicants had published copies of the documents, which had previously been sent to them anonymously, and had been convicted for doing so. The European Court of Human Rights ruled that informing the public about the level of remuneration contributed to the public debate about the wages paid by the company taking place at that time in the context of collective bargaining negotiations. The decisive factor for the Court's decision was, however, that under French law the information contained in the documents was publicly accessible to taxpayers living in the same tax district. In addition, the salaries of the top executives of big companies like Peugeot were, the Court pointed out, regularly published in financial magazines, and the fundamental legality of the publication of that information was undisputed. A conviction solely on the ground that the documents as such were published constituted a violation of press freedom.[62]

Fifteen years previously, the German Federal Constitutional Court ruled in a constitutional complaint filed by the publishers Axel Springer AG against the investigative journalist Günter Wallraff that the publication of unlawfully procured or obtained information was also protected by freedom of expression. However, information could not be published when the reporter had obtained it "unlawfully through deception" and intended to use it "for an attack on the person deceived". An exception to that applied only "when the importance of the information for informing the public and enabling it to form an opinion clearly outweighs the disadvantages that the breach of the law must entail for the person concerned and for the (actual) validity of the legal order". That case, the Court noted, "normally" did not arise when the information referred to conditions or behaviour that were not in themselves unlawful.[63]

60) Cf. Steven Swinford, "Hyper-injunction" stops you talking to MP, 21 March 2011, http://www.telegraph.co.uk/news/uknews/law-and-order/8394566/Hyper-injunction-stops-you-talking-to-MP.html
61) ECHR, *Fressoz and Roire v. France* judgment of 21 January 1999, Application No. 29183/95.
62) The Italian lower house came to a different conclusion in 2010: following the publication of police reports on intercepted telephone conversations of the Prime Minister, it approved a bill on 10 June 2010 that provides for the imposition of significant limits on telephone tapping and the publication of wiretap reports and would even make quoting from investigation files a punishable offence. For a detailed analysis of the background to this discussion, see also Michael Braun, "Abhörprotokolle belegen Manipulation", available at http://www.taz.de/!7966/ , and APA report entitled "Rechtsanwälte bestreiten Berlusconis Verwicklung in Fernsehaffäre", derstandard.at, 20 July 2011, http://derstandard.at/1310511702569/Italien-Rechtsanwaelte-bestreiten-Berlusconis-Verwicklung-in-Fernsehaffaere . This would considerably limit the possibility of reporting on criminal proceedings. Having been amended by the Senate, the bill is now once again before the lower house; see, the Stenographic Record of Chamber of Deputies sitting no. 529 of 5 October 2011, pp. 1 ff., http://www.camera.it/412?idSeduta=529&resoconto=stenografico&indice=alfabetico&tit=00040&fase=#sed0529.stenografico.tit00040
63) BVerfGE 66, 116 (quoted from http://www.servat.unibe.ch/dfr/bv066116.html).

© 2011, European Audiovisual Observatory, Strasbourg (France)

The cases described above concerned the processing of unlawfully obtained data by publishing them in the media.

It is interesting that the Data Protection Directive does not in principle distinguish between whether the data were or are public or private. In *Satakunnan et al.*, the Advocate-General argued that the right to privacy usually gives way to freedom of expression in the case of details already published. However, the person concerned may be protected from any further processing and dissemination, for example in the case of erroneous information, libel or information concerning intimate matters. Member states' margin of discretion "cannot lead to the legitimation of manifestly disproportionate interference in the right to privacy".[64]

The publication of a video in a Web 2.0 environment was considered by a court in Milan in 2010,[65] which had to decide whether four Google executives had committed a criminal offence for failing over a period of several weeks to delete a video showing the maltreatment of a person with Down's Syndrome. The accused considered their platform Google Video to be no more than a hosting provider that was not liable for the uploaded content,[66] stating that anyone who uploaded videos was bound by its terms and conditions, including the provisions on the protection of privacy. The court agreed with their argument that a provider that merely made a "connection service" available was not obliged to check the uploaded content. However, the provider did have to inform its users about their obligations with regard to respect for personality rights. In particular, the court criticised the fact that the person shown had not consented to the publication of his personal data. Although Google might not be able to check whether consent had been given in every individual case, the company should at least ensure that the user uploading the content, who at the same time acted as a content provider (known in this dual role as a "prosumer"), confirmed that such consent had been obtained. That could for example be done by means of a data protection notice that was always displayed before a video was uploaded and required the user to confirm it had been read.[67]

III. Media and the Protection of User Data

Personal data also play a role in the relationships between the media and their users. In contrast to when data are processed for journalistic purposes, the media employ user data for marketing content. Here (as in all other non-journalistic relations), they have to comply with the data protection rules.[68] In addition to the "general" Data Protection Directive 95/46/EC, Directive 2002/58/EC[69] contains special provisions on data protection in electronic communications. In the context of the so-called "Telecoms Review",[70] the directive was modified by amendments, which

64) Advocate-General's Opinion in the *Satamedia* case, op. cit., para. 124.
65) Valentina Moscon, "The Italian Google Verdict", IRIS 2010-6:1/35.
66) Cf. Article 14 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), OJ EC of 17 July 2000, L 178, p. 1.
67) However, a German court held that the operator of a forum via which a user had published personal data of a third party that were publicly accessible in the Irish Register of Companies was itself responsible for the data processing because making the forum contributions available was at least in "its own business interests" (see OLG Hamburg (Hamburg Court of Appeal), judgment of 2 August 2011, 7 U 134/10, quoted from http://www.aufrecht.de/index.php?id=6988). However, the operator was allowed to make the contribution available for retrieval in the case in issue because it had been established that there was a public interest in obtaining the information for the purposes of consumer education, an interest that justified the disclosure of the data pursuant to Article 28(2) of the Federal Data Protection Act. The same conclusion, the court went on, resulted from weighing freedom of expression against general personality rights.
68) For a detailed discussion of the situation under British law, see *Ian Walden/Lorna Woods*, "Broadcasting Privacy", Journal of Media Law 2011 (Vol. 3, No. 1), pp. 117 ff.
69) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ EC of 31 July 2002, L 201, p. 37.
70) See on this Sebastian Schweda, "The 'Telecoms Review': New Impetus for Audiovisual Media?", European Audiovisual Observatory (publ.), *Communications Regulation: Between Infrastructure and Content*, IRIS *plus* 2009-10.

© 2011, European Audiovisual Observatory, Strasbourg (France)

are contained in Directive 2009/136/EC.[71] These included Article 5(3) of Directive 2002/58/EC, according to which information, such as cookies, may only be stored on or retrieved from the user's terminal with his or her consent. The specific impact of these provisions on the activities of the media when they make content available and market it is discussed below.

1. Traditional Media

The media consumer is the subject of diverse forms of data processing. Although the completely anonymous use of media is technically possible, such as in the case of a newspaper purchase at a newsstand or the free-to-air reception of programmes broadcast terrestrially or by satellite, marketing models involving the processing of the customer's personal data are often employed for practical or legal reasons. Those who want to have their daily newspaper delivered to their home must at least provide their name and address. The choice of specific distribution channels, such as cable television, presupposes a contractual relationship with transmission service providers (i.e., cable network and/or platform operators), which need their customers' details to provide and bill the service.[72]

However, content providers also often depend on these data: if the business model provides for the financing of a media offering by the user, it must be possible to identify that person. If the fee varies according to the actual extent of the use (as in the case of pay-per-view services, for example), it is also necessary to process use-dependent data (traffic data[73]). The same applies to audiovisual services that offer additional interactive functions and therefore must have a return channel that transmits information from the user to the service provider. An example of this is so-called "Connected TV".[74]

In some states, the (potential) recipient of public service broadcasts contributes to their financing. If the obligation to pay depends on certain preconditions, personal data also have to be processed in order to find out which citizens are required to pay and whether they actually meet their financial commitments. In principle, this applies both to the recipient's obligation to pay fees and to a household levy.[75]

2. "New" Media

a) Technical bases of data processing and legal classification

In order to make media content available, the data processing may in many cases be limited to user data, and an evaluation of the usage behaviour is only necessary when the fee for the access is calculated according to the nature and extent of the use. This also applies in principle to the "new" media offered via digital communications networks. However, the use of packet-switched data transmission, for example Internet or other IP based networks, requires and permits the identification of any communication terminal via a distinct address. This ensures that an item

71) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ EU of 18 December 2009, L 337, p. 11.
72) Personal data means the data (within the meaning of Article 2(a) DPD, cf. ZOOM, section II. 2. a)) that identify the user or subscriber and have to be processed by the service provider for the purpose of implementing the contract, such as the person's name and address and, as the case may be, bank account details.
73) See the definition in Article 2(b) of Directive 2002/58/EC, according to which traffic data are "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".
74) See on this Sebastian Artymiak, "Introduction to Different Forms of On-demand Audiovisual Services, in: IRIS Special, The Regulation of On-demand Audiovisual Services: Chaos or Coherence?, European Audiovisual Observatory (publ.), Strasbourg 2011 (forthcoming).
75) Cf. Christian M. Bron, "Financing and supervision of public service broadcasting", in: European Audiovisual Observatory (publ.), *Public Service Media: Money for Content*, IRIS *plus* 2010-4.

© 2011, European Audiovisual Observatory, Strasbourg (France)

of information finds the path from the sender to the recipient. In order to rule out transmission errors as far as possible, each data package received error-free must be confirmed by the recipient. This means that the terminal that receives content and the time period of reception can already be established when the information is transmitted.[76]

Against this background, vertically integrated companies that act both as content providers and Internet access providers or platform operators (such as IPTV providers, which market their service via their company's own DSL access) are able to link customer, traffic and usage data.[77] User profiles produced in this way provide information on what content from the company's media offering has been retrieved using what connection and at what time.

In contrast to the traditional transmission channels, bidirectional communication channels provide their own return path: the provision of interactive television or media consumption on demand (e.g., video on demand) is made considerably easier by packet-switched data transmission. Individual users are only given access to the content if they at least identify themselves to their network operator. This also applies when the services are offered using the multicast method.[78] For mobile use, linear television services are often transmitted via digital broadcasting transmission technologies belonging to the DVB family. In the case of these transmission standards, there is no bidirectional communication but classical broadcasting in the sense of a signal sent "to everyone". Additional interactive services can be used if a combined terminal that also provides access to a (GSM/UMTS) mobile telephone network is employed. Via this network, the user has a return channel available in the same terminal. On the other hand, if audiovisual content is retrieved via UMTS or other wireless Internet access services (GPRS, Wi-Fi, WiMax), the transmission of the television signals is based on a bidirectional communications link.

On lower and higher protocol layers (based on the OSI layer model), the use of the media service often generates additional data that permit the user to be identified, for example even after changing the IP address. Especially on the application layers, assignment to a terminal is possible via so-called (HTTP or browser) cookies, which have been used for a long time: a website called up by the user deposits a file on the computer and can read it again when it is revised by the user on this or another company website. "Flash cookies" employed using the widespread "Flash" technology to display audiovisual content also enable the usage to be tracked from a particular computer. Finally, according to a study[79] website operators – including until recently the US video portal *Hulu.com* and the music service *spotify.com* – employ still largely unknown technologies to restore deleted cookies (so-called "cookie respawning") and enable the browser to be identified over a particularly long period (so-called "persistent cookies").

Additional information is available by "reading" the browser and system configuration used, details of which the browser transmits with every page request and in many cases enables the terminal to be localised very precisely. By comparing the Internet pages previously visited via that terminal with a list of known websites, which is possible with a number of browsers, a website operator can also establish whether a user has already called up the services offered by its

76) In the *Promusicae* case, the Advocate-General at any rate classified dynamic IP addresses as traffic data and (at least) the information linking the IP address to the subscriber as personal data (see the Advocate-General's Opinion of 18 July 2007, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, paras. 61 and 63).

77) Based on section 15 of the German Telemedia Act, these are a user's personal data required to receive and bill a media service, i.e. for example details identifying the user, usage times and information on the content retrieved.

78) In the case of multicasting, content is transmitted from a sender to several recipients. Unlike a point-to-point connection between two terminals, the signal in the case of a multicast is sent only once but can be received by several subscribers. In contrast to broadcasting, however, it is not enough to select the relevant transmission channel on a reception device switched on for the purpose. Rather, it is first necessary to "dial in" to the transmission service provider.

79) See abstract at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390 . The technologies used are mainly based on the storage (caching) of the cookie information in other storage sectors of the local computer accessible to the browser. If an HTTP cookie of a page that uses these technologies is deleted, its information can be read, e.g. by JavaScript, from the other storage sectors and the HTTP cookie restored without the user knowing or consenting to this.

© 2011, European Audiovisual Observatory, Strasbourg (France)

competitors.[80] Tracking tools like Google Analytics enable a provider to carry out a user-specific analysis of access to its own website. Opinions on the legality of such tools vary.[81]

According to the OSI model, below the "network layer", on which the Internet Protocol ensures the onward transmission of the data packages, is the data link layer, on which access to network adapters is controlled via internationally unique, device-specific so-called "MAC addresses".[82] For some time, Google has been collecting the MAC addresses of the base stations of short-range wireless networks (Wireless Local Area Networks – WLANs) worldwide both during its journeys for the Street View picture service and with the help of Android smartphones. The purpose of this is to enable mobile telephone users to find out their own position without GPS. In June 2011, it was reported that some MAC addresses of private computers and smartphones had been entered into the database.[83]

Owing to users' close link to their devices (especially their mobile devices), both the EDPS and the Article 29 Data Protection Working Party consisting of representatives of data protection authorities regard the geolocation of MAC addresses as personal data. The Article 29 Data Protection Working Party calls for sufficient guarantees to ensure an appropriate balance of interests for those affected by data processing, such as an easy and permanent opt-out without their needing to provide additional personal data. Moreover, it is not necessary to process the so-called "Single Station Identifier" (SSID) of a Wi-Fi hotspot for the purpose of offering geolocation services.[84]

b) Private business interests in using the data and the relevant legal framework

The data processed to make the content available can be used for various purposes that go beyond merely providing a guarantee of proper access to the service. Content providers in particular have a vital interest in using the data as they often need them for billing paid services.

However, there are also commercial interests in using data in the case of services offered free of charge: media services on the Internet are often financed exclusively by advertising. In return for their financial contribution, advertisers expect their clientele to be reached in as targeted a way as possible. The identification of users in package-based networks and the monitoring of their activities over a long period enable user profiles to be produced and can be employed for advertising tailored to individual interests. As behaviour-oriented advertising is considered more likely to hold out prospects of success than non-target-group-specific advertising, the advertising medium can usually generate higher revenues with it.[85]

In the context of data protection law, this form of advertising, for which the term "online behavioural advertising" (OBA) has become established, encounters a number of misgivings. The EDPS described the systematic use of such techniques as a "highly intrusive practice".[86] He deplored in this connection the "erosion of fundamental rights and a market failure", going on to say that "certain public interests have apparently not been sufficiently included in the way the internet has

80) Cf. on this Dongseok Jang et al., "An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications", available at http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf
81) See Thomas Hoeren, Google Analytics – datenschutzrechtlich unbedenklich?, *ZD* 2011, 3 ff. and, most recently, http://www.sueddeutsche.de/digital/umstrittener-web-statistikdienst-datenschuetzer-erlaubt-einsatz-von-google-analytics-1.1144297
82) MAC stands here for Media Access Control.
83) Cf. "WLAN-MAC-Adressen: Googles langes Gedächtnis", 16 June 2011, http://www.heise.de/netze/meldung/WLAN-MAC-Adressen-Googles-langes-Gedaechtnis-1261893.html
84) Article 29 Data Protection Working Party, Opinion 13/2011 of 16 May 2011 on Geolocation services on smart mobile devices, WP 185, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf , p. 17.
85) On the basic technical and economic conditions, see Opinion 2/2010 of 22 June 2010 on Online Behavioural Advertising, Doc. WP 171 of the Article 29 Data Protection Working Party p. 4 f, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf
86) EDPS, lecture on 7 July 2011 at the University of Edinburgh School of Law: "Do not track or right on track? – The privacy implications of online behavioural advertising", available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_EN.pdf , p. 7.

© 2011, European Audiovisual Observatory, Strasbourg (France)

developed so far". To redress this unacceptable state of affairs, he called for corrective legal, self-regulatory[87] and technical measures.

Advertisers can appeal to target groups not only by advertising in third-party offerings but also via their own services. The following campaign by the American brewery Budweiser recently attracted considerable attention: on its British Facebook page, the company showed a match in August 2011 involving the less well-known football club Ascot United. Anyone wanting to see the game had to click the "Like" button.[88]

By means of this button, registered Facebook users can publicly indicate their support for the content of a page or its provider. The main problem here from the data protection point of view is that the data of users not registered with Facebook who visit a website with such a button integrated into it can also be processed.

However, it is already a contentious issue whether EU data protection law is at all applicable to data processing by US companies such as Facebook. If this is declared to be the case, the applicable law will continue to be discussed. Does the law of Ireland, where Facebook's European headquarters are located, apply or that of the country in which the user is staying or residing?[89] Whatever the case, the *Unabhängiges Landeszentrum für Datenschutz* in Schleswig-Holstein (Independent Regional Data Protection Centre – ULD) has now turned its attention to content providers who use the "Like" button on their web pages: according to their working paper, the insertion of the button into websites hosted in Germany breaches both German and European data protection law.[90] The ULD also severely criticises a violation of Article 5(3) of Directive 2002/58/EC, stating that merely looking through a website containing the button caused cookies to be installed and the IP address, browser-specific information and other data to be processed without the user's effective consent. The authority called on the website operators concerned to remove the button by the end of September 2011, failing which fines of up to EUR 50 000 could be imposed.

Especially with regard to the use of cookies and other measures to store information in, or retrieve information from, the user's terminal Article 5(3) of Directive 2002/58/EC provides:

> "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his/her consent."

The consent can only be dispensed with when the storage or access takes place for the sole purpose of transmitting a communication over an electronic communications network or if this is

---

87) There are initiatives of the European Advertising Standards Alliance (see "EASA Best Practice Recommendation on Online Behavioural Advertising", 13 April 2011, http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download) and the Interactive Advertising Board Europe ("IAB Europe EU Framework for Online Behavioural Advertising", http://www.iabeurope.eu/media/51925/iab%20europe%20oba%20framework_merged%20ii.pdf). However, the EDPS considers these initiatives insufficient, at least with regard to the use of cookies, as they would implement the present opt-out model rather than the opt-in approach favoured by Directive 2009/136/EC (cf. lecture of 7 July 2011 (see previous footnote), p. 6). The Article 29 Data Protection Working Party also criticises the initiatives as insufficient (see its letter of 3 August 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf). From the youth protection point of view, a number of social network providers, including Facebook, MySpace and YouTube, have undertaken to make the settings for the protection of privacy easy to locate and accessible and to establish the default setting for the profiles of minors as "private". Cf. "Social Networking: Commission brokers agreement among major web companies", press release of 10 February 2009, IP/09/232, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/232&format=HTML&aged=1&language=EN&guiLanguage=en

88) Cf. Johannes Kuhn, "Provinzgekicke vor Millionen Zuschauern – Facebook entdeckt den Fußball", 18 August 2011, http://www.sueddeutsche.de/digital/englische-pokalbegegnung-im-live-stream-facebook-sorgt-fuer-fussballrausch-in-der-provinz-1.1132389

89) See on this question Thomas Stadler, "Gilt deutsches Datenschutzrecht für Facebook überhaupt?", 18 August 2011, http://www.internet-law.de/2011/08/gilt-deutsches-datenschutzrecht-fur-facebook-uberhaupt.html . Stadler considers German law to be applicable to the processing of German users' personal data by Facebook.

90) ULD, "Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook", 19 August 2011; available at https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf

© 2011, European Audiovisual Observatory, Strasbourg (France)

absolutely necessary for the provision of a service. Furthermore, Article 5(3) of Directive 2002/58/EC provides that the subscriber must be given clear and comprehensive information in accordance with the Directive, especially about the purposes of the processing. The consent may in principle be given "by any appropriate method enabling a freely given specific and informed indication of the user's wishes".[91]

With regard to the practical implementation of these requirements, the EDPS suggests[92] enabling the consent declaration to be made via the browser settings, as expressly permitted by Recital 17 of Directive 2002/58/EC. In the view of the EDPS, a solution should be both "user friendly *and* effective". The EU Commissioner for the Digital Agenda had previously praised the "do-not-track" model based on an opt-out, which is implemented in some more recent browsers. The EDPS criticised this attitude and called for the inclusion of a "privacy wizard" in the browser software to ensure that users are able to select the data protection settings in accordance with their preferences. In addition, the default settings should prevent the storing of cookies of third-party providers as long as the user does not explicitly decide otherwise. This idea, referred to as "privacy by default", could in principle also be applied with other forms of OBA involving recourse to certain hardware and software configurations (e.g., hardware digital decoder or proprietary TV software).

IV. Future Developments

It is basically become less and less complicated for the individual to obtain a media presence. In particular, the Internet has made it much easier to convey information to a potentially unlimited group of people not known in advance. Today, the establishment of a "mass medium" (blogs, Facebook page) no longer constitutes a real organisational, technical or financial hurdle, especially owing to the (mostly free) aids provided for this. With the help of search engines and instruments, locating the information made available is no longer dependent on media content aggregators, such as press publishers and broadcasters, which provide users with a well-known platform and make it easier for them to find information.

However, the bodies mentioned traditionally not only compile (their own and third-party) content and make it accessible. Rather, their particular feature is that they assume editorial responsibility for the information. In their editorial activities, which, in particular, comprise gathering, checking, weighting, classifying, preparing and marshalling data, they are subject to legal and/or self-regulatory duties of care and thus have corresponding specific rights. It is questionable whether it can in principle be assumed that individuals who publish content on Facebook or in the relevant media actually undertake these tasks. At any rate, the standard of care applied to the classical media is usually not applied to their activities.

If the member states give a wide interpretation – as demanded by the ECJ – to the possibility provided for in Article 9 DPD of introducing exemptions for data processing carried out for journalistic purposes, then any individual who engages in a journalistic activity can in principle enjoy this privilege. However, it is doubtful that European states agree on what data protection obligations an individual "prosumer" can be exempted from.[93] There is (still) a lack of clear criteria on structuring and shaping the process of weighing the right to the protection of personal data (and, more generally, the personality) against freedom of the media. This may have something to do with the cultural differences between member states. As we have seen, Scandinavian countries seem to assess the need for protection in the case of income-related data, for example, differently from countries like Germany.[94] On the other hand, ideas on what constitutes journalism evidently

91) Cf. Recital 17 of Directive 2002/58/EC.
92) EDPS, op. cit. (fn. 86), p. 5 f.
93) See on the discussion of this subject in Canada http://knightcenter.utexas.edu/blog/quebec-pushing-forward-controversial-proposal-define-professional-journalists
94) Tax confidentiality, breaches of which are subject to criminal penalties (section 30 of the Revenue Code [*Abgabenordnung*]) only permits the disclosure of tax data by officials in very few exceptional cases.

© 2011, European Audiovisual Observatory, Strasbourg (France)

also differ considerably, so we are justified in doubting that the revision of the DPD can bring about the greater harmonisation of Article 9.

At the moment, it also seems uncertain whether the focus will remain on the original disseminator of the information or whether the role of those who enable access to it, such as search engines or the providers of links, will also be examined. Will they also be classified as controllers and, if so, with what rights and obligations? At this point, it is necessary (once again) to consider the E-Commerce Directive and the limitations on liability it contains and perhaps find a way of striking a proper balance with the right to data protection.

As shown, the developments in the new media also give cause to address the subject of the protection of users' personal data. In addition to the services offered by professional media companies, this once again concerns the content that any individual can make available, with or without the use of professional platforms such as YouTube or Facebook. The issue of data protection has several different facets here, too. A particularly crucial aspect will probably be the "sandwich" situation that non-professional providers frequently get themselves into: if they use a professional platform to make their media content available, then a relationship with its provider of relevance to data protection legislation comes about. At the same time, the protection of personal data also becomes relevant in the relationship with the users of the information they have published. The fundamental question as to the prosumer's responsibility, especially in the latter situation, still seems to have remained largely unanswered.[95] In this context, an important role is likely to be played by the considerable uncertainty about the prosumer's knowledge of the platform's internal data processing processes and what possibilities he or she may have of influencing them.

It therefore remains very interesting to see what possible solutions to the many issues involving the media and data protection are discussed and pursued, especially in connection with the revision of the legal instruments of the EU and the Council of Europe.

95) At least when the prosumer is also the operator of the website via which the content that he or she has produced is made available, he or she must – as the individual with access to the technical systems for processing the data – comply vis-à-vis the users of that "media offering" with all data protection rules applicable to the data processing in connection with the provision of the service. In the European legal context, this means that either the consent of the person concerned or a legal basis is required.

© 2011, European Audiovisual Observatory, Strasbourg (France)

Balancing Conflicting Interests

Matters relating to the legality of limiting freedom of expression are regularly on the agenda of the European Court of Human Rights, which in many cases also deals with the question of the extent to which the very interest in the protection of privacy permits interference with the rights enshrined in Article 10 of the Convention. The core issues here are such delicate subjects as the prior censorship of media services or irreparable damage to an individual's reputation and private life. Domestic courts also deal with these issues from various points of view. The first part of the Related Reporting accordingly not only discusses the Court's most recent decisions but also the German "media privilege" and a rule on the protection of minors contained in the French Civil Code.

However, court decisions are only the last resort to bring about a balance between freedom of expression and the protection of data. A possible alternative is the right of reply, which can contribute to settling a dispute about the protection of data and is the focus of the second part of Related Reporting. Ideally, however, players are so aware of the issues involved in handling private data that clashes of interests are avoided from the outset. This prevention through self-regulation is the subject of the third part of Related Reporting. Finally, we have added a fourth part, which discusses in very broad terms the regulation of the Internet or how to avoid it. The related question is whether the Internet should be given special treatment regarding the use of personal data.

© 2011, European Audiovisual Observatory, Strasbourg (France)

Limits to the Freedom of Information and Expression

European Court of Human Rights

RTBF v. Belgium

Dirk Voorhoof
Ghent University (Belgium) & Copenhagen University (Denmark)
& Member of the Flemish Regulator for the Media

In a judgment of 29 March 2011 the European Court found a violation of Article 10 of the European Convention on Human Rights in the case Radio-télévision belge de la communauté française (RTBF) v. Belgium. The case concerned an interim injunction ordered by an urgent-applications judge against the RTBF, preventing the broadcasting of a programme on medical errors and patients' rights. The injunction prohibited the broadcasting of the programme until a final court decision in a dispute between a doctor named in the programme and the RTBF. As the injunction constituted an interference by the Belgian judicial authorities with the RTBF's freedom of expression, the European Court in the first place had to ascertain whether that interference had a legal basis. Whilst Article 10 does not prohibit prior restraints on broadcasting, such restraints require a particularly strict legal framework, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse. As news is a perishable commodity, delaying its publication, even for a short period, might deprive it of all its interest.

In ascertaining whether the interference at issue had a legal basis, the Court observed that the Belgian Constitution authorised the punishment of offences committed in the exercise of freedom of expression only once they had been committed and not before. Although some provisions of the Belgian Judicial Code permitted in general terms the intervention of the urgent-applications judge, there was a discrepancy in the case law as to the possibility of preventive intervention in freedom of expression cases by that judge.

The Belgian law was thus not clear and there was no constant jurisprudence that could have enabled the RTBF to foresee, to a reasonable degree, the possible consequences of the broadcasting of the programme in question. The European Court observed that, without precise and specific regulation of preventive restrictions on freedom of expression, many individuals fearing attacks on them in television programmes – announced in advance – might apply to the urgent-applications judge, who would choose different solutions to their cases and that this would not be conducive to preserving the essence of the freedom of imparting information. Although the European Court considers a different treatment between audiovisual and print media not unacceptable as such, e.g., regarding the licensing of radio and television, it did not agree with the Belgian Court of Cassation decision to refuse to apply the essential constitutional safeguard against censorship of broadcasting. According to the European Court, this differentiation appeared artificial, while there was no clear legal framework to allow prior restraint as a form of censorship on broadcasting. The Court was of the opinion that the legislative framework, together with the case-law of the Belgian courts, did not fulfil the condition of forseeability required by the Convention. As the interference complained of could not be considered to be prescribed by law, there had thus been a violation of Article 10 of the Convention. The judgment contains an important message to all member states of the European Convention on Human Rights: prior restraints require a particularly strict, precise and specific legal framework, ensuring both tight control over the scope of bans both in print media and in audiovisual media services, combined with an effective judicial review to prevent any abuse by the domestic authorities.

- Judgment by the European Court of Human Rights (Second Section), case of RTBF v. Belgium (no. 50084/06) of 29 March 2011
  http://merlin.obs.coe.int/redirect.php?id=13171

IRIS 2011-6/1

© 2011, European Audiovisual Observatory, Strasbourg (France)

Mosley v. the United Kingdom

Dirk Voorhoof
Ghent University (Belgium) & Copenhagen University (Denmark)
& Member of the Flemish Regulator for the Media

In the case Mosley v. the United Kingdom the European Court of Human Rights decided that the right of privacy guaranteed by Article 8 of the European Convention on Human Rights does not require the media to give prior notice of intended publications to those who feature in them. The applicant in this case is Max Rufus Mosley, the former president of the International Automobile Federation. In 2008, the Sunday newspaper News of the World published on its front page an article entitled "F1 Boss Has Sick Nazi Orgy with 5 Hookers", while several pages inside the newspaper were also devoted to the story and included still photographs taken from video footage secretly recorded by one of the participants in the sexual activities. An edited extract of the video, in addition to still images, were also published on the newspaper's website and reproduced elsewhere on the Internet. Mr Mosley brought legal proceedings against the newspaper claiming damages for breach of confidence and invasion of privacy. In addition, he sought an injunction to restrain the News of the World from making available on its website the edited video footage. The High Court refused to grant the injunction because the material was no longer private, as it had been published extensively in print and on the Internet. In subsequent privacy proceedings the High Court found that there was no public interest and thus no justification for publishing the litigious article and accompanying images, which had breached Mr. Mosley's right to privacy. The court ruled that News of the World had to pay to Mr. Mosley 60,000 GBP in damages.

Relying on Article 8 (right to private life) and Article 13 (right to an effective remedy) of the European Convention, Mr. Mosley complained that, despite the monetary compensation awarded to him by the courts, he remained a victim of a breach of his privacy as a result of the absence of a legal duty on the part of the News of the World to notify him in advance of their intention to publish material concerning him, thus giving him the opportunity to ask a court for an interim injunction and prevent the material's publication. The European Court found indeed that the publications in question had resulted in a flagrant and unjustified invasion of Mr. Mosley's private life. The question which remained to be answered was whether a legally binding pre-notification rule was required. The Court recalled that states enjoy a certain margin of appreciation in respect of the measures they put in place to protect people's right to private life. In the United Kingdom, the right to private life is protected with a number of measures: there is a system of self-regulation of the press; people can claim damages in civil court proceedings; and, if individuals become aware of an intended publication touching upon their private life, they can seek an interim injunction preventing publication of the material. As a pre-notification requirement would inevitably also affect political reporting and serious journalism, the Court stressed that such a measure would require careful scrutiny. In addition, a parliamentary inquiry on privacy issues had been recently held in the UK and the ensuing report had rejected the need for a pre-notification requirement. The Court further noted that Mr. Mosley had not referred to a single jurisdiction in which a pre-notification requirement as such existed nor had he indicated any international legal texts requiring states to adopt such a requirement. Furthermore, as any pre-notification obligation would have to allow for an exception if the public interest were at stake, a newspaper would have to be able to opt not to notify an individual if it believed that it could subsequently defend its decision on the basis of the public interest in the information published. The Court observed in that regard that a narrowly defined public interest exception would increase the chilling effect of any pre-notification duty. Anyway, a newspaper could choose, under a system in which a pre-notification requirement was applied, to run the risk of declining to notify, preferring instead to pay a subsequent fine. The Court emphasised that any pre-notification requirement would only be as strong as the sanctions imposed for failing to observe it. But at the same time the Court emphasised that particular care had to be taken when examining constraints which might operate as a form of censorship prior to publication. Although punitive fines and criminal sanctions could be effective in encouraging pre-notification, they would have a chilling effect on journalism, including political and investigative reporting, both of which attract a high level of protection under the Convention. Such as scheme would therefore run the risk of being incompatible with the Convention's requirements of freedom

© 2011, European Audiovisual Observatory, Strasbourg (France)

of expression, guaranteed by Article 10 of the Convention. Having regard to the chilling effect to which a pre-notification requirement risked giving rise, to the doubts about its effectiveness and to the wide margin of appreciation afforded to the UK in this area, the Court concluded that Article 8 did not require a legally binding pre-notification requirement.

- Judgment by the European Court of Human Rights (Fourth Section), case of Mosley v. United Kingdom, No. 48009/08 of 10 May 2011, http://merlin.obs.coe.int/redirect.php?id=13310

IRIS 2011-7/1

Sigma Radio Television Ltd. v. Cyprus

Dirk Voorhoof
Ghent University (Belgium) & Copenhagen University (Denmark)
& Member of the Flemish Regulator for the Media

This case concerns a complaint by a broadcasting company regarding a number of decisions by the Cyprus Radio and Television Authority (CRTA) imposing fines on the company for violations of legislation concerning radio and television programmes in its broadcasts and the alleged unfairness of the related domestic proceedings. The breaches found by the CRTA concerned advertisements for children's toys; the duration of advertising breaks; the placement of sponsors' names during news programmes; product placement in a comedy series; news programmes that lacked objectivity or contained material unsuitable for minors or were disrespectful of crime victims and their relatives; films, series and trailers that contained offensive remarks and inappropriate language or included scenes of violence unsuitable for children; and, in one particular case, racist and discriminatory remarks in an entertainment series.

Sigma RTV alleged substantially that it had been denied a fair hearing before an independent and impartial tribunal, invoking Article 6 of the Convention.
[...]

The Court came to the conclusion that Sigma RTV's allegations as to shortcomings in the proceedings before the CRTA, including those concerning objective partiality and the breach of the principles of natural justice, were subject to review by the Supreme Court and that the scope of the review of the Supreme Court in the judicial review proceedings in the present case was sufficient to comply with Article 6 of the Convention.

The Court also dismissed Sigma RTV's complaints regarding the alleged violation of Article 10 of the Convention as all decisions by the CRTA were in accordance with Art. 10 §2, the sanctions and fines being prescribed by law, being proportionate and being pertinently justified on the basis of legitimate aims. These aims, in general, included [...] the need for a fair and accurate presentation of facts and events and the protection of the reputation, honour, good name and privacy of persons involved in or affected by the broadcast. The Court found therefore, that the interference with Sigma RTV's exercise of their right to freedom of expression in these cases can reasonably be regarded as having been necessary in a democratic society for the protection of the rights of others. The Court accordingly declared inadmissible, as manifestly ill-founded, Sigma RTV's complaints under Article 10 in respect of the CRTA's decisions. One complaint however received a more thorough analysis on the merits: the complaint regarding the racist and discriminatory content of a fictional series. The Court emphasises that it is particularly conscious of the vital importance of combating racial and gender discrimination in all its forms and manifestations and that the CRTA could not be said in the circumstances to have overstepped its margin of appreciation in view of the profound analysis at the national level, even though the remarks had been made in the context of a fictional entertainment series. Lastly, as to the proportionality of the impugned measure, the Court found,

© 2011, European Audiovisual Observatory, Strasbourg (France)

bearing in mind the amount of the fine and the fact that the CRTA, when imposing the fine, took into account the repeated violations by the applicant in other episodes of the same series, that the fine imposed (approximately EUR 3,500) was proportionate to the aim pursued. Accordingly, there has been no violation of Article 10 of the Convention.

Finally the Court also dismissed the complaint regarding the alleged discrimination against Sigma RTV, operating as a private broadcaster under stricter rules, restrictions and monitoring than the national public broadcasting company in Cyprus, CyBC. [...]

- Judgment by the European Court of Human Rights (Fifth Section), case of Sigma Radio Television Ltd. v. Cyprus, Nos. 32181/04 and 35122/05 of 21 July 2011
  http://merlin.obs.coe.int/redirect.php?id=13402

IRIS 2011-8/3

Sipoș v. Romania

Dirk Voorhoof
Ghent University (Belgium) & Copenhagen University (Denmark)
& Member of the Flemish Regulator for the Media

In a remarkable judgment the European Court of Human Rights has come to the conclusion that Romania breached the right of privacy of a journalist when the Romanian courts acquitted the director and the coordinator of the press office of the Romanian Television Company (SRTV) in criminal defamation and insult proceedings.

At the heart of the case lies a press release published by the management of the Romanian State TV channel, after removing the applicant, Ms. Maria Sipoş, from a programme that she produced and presented on the National State channel România 1. Following her replacement as a presenter, Ms. Sipoş made a number of statements to the press alleging that SRTV was engaged in censorship. The broadcaster responded in turn by issuing a press release, explaining that Ms. Sipoş had been replaced due to audience numbers. The press release, quoted by six national newspapers, also made reference to Ms. Sipoş' emotional state due to family problems, it questioned her discernment, referred to allegedly antagonistic relations between her and her colleagues and suggested she was a victim of political manipulation. Ms. Sipoş claimed that SRTV's press release had infringed her right to her reputation, and she brought criminal proceedings before the Bucharest District Court against the channel's director and the coordinator of the SRTV's press office, accusing both of insults and defamation. The Bucharest County Court acknowledged that the press release contained defamatory assertions about Ms. Sipoş, but having regard to the fact that the defendants had not intended to insult or defame her and in view of their good faith, it dismissed Ms. Sipoş' claims.

Before the European Court of Human Rights Ms. Sipoş complained that the Romanian authorities had failed in their obligation, under Article 8 of the Convention, to protect her right to respect for her reputation and private life against the assertions contained in the press release issued by the SRTV. Referring to the positive obligations a State has in securing respect for private life, even in the sphere of relations between private individuals, the European Court clarified that it had to determine whether Romania had struck a fair balance between, on the one hand, the protection of Ms. Sipoş' right to her reputation and to respect for her private life, and on the other, the freedom of expression (Article 10) of those who had issued the impugned press release. For that purpose the Court examined the content of the press release and found, in particular, that the assertions presenting Ms. Sipoş as a victim of political manipulation were devoid of any proven factual basis, since there was no indication that she had acted under the influence of any particular vested interest. As regards the remarks about her emotional state, the Court noted that they were based on

© 2011, European Audiovisual Observatory, Strasbourg (France)

elements of her private life whose disclosure did not appear necessary. As to the assessment about Ms. Sipoş' discernment, it could not be regarded as providing an indispensable contribution to the position of the SRTV, as expressed through the press release, since it was based on elements of the applicant's private life known to the SRTV's management. The Court noted that, given the chilling effect of criminal sanctions, a civil action would have been more appropriate, but it concluded nonetheless that the statements had crossed the acceptable limits and that the Romanian courts had failed to strike a fair balance between protecting the right to reputation and freedom of expression. Thus, there had been a violation of Article 8, and Ms. Sipoş was awarded EUR 3,000 in damages.

One dissenting judge, Judge Myer, drew attention to a particular issue in this case. Although the Third Chamber of the Court recognized that criminal sanctions have a chilling effect on speech and that it would have been more appropriate to initiate the civil proceedings available to the applicant, nevertheless the majority of the European Court found that the criminal sanction of the director and press officer of the SRTV was necessary in a democratic society in order to protect Ms. Sipoş' right to her reputation and private life, an approach that contrasts with Resolution 1577(2007) of the Parliamentary Assembly of the Council of Europe urging the decriminalization of defamation and insult.

- Judgment by the European Court of Human Rights (Third Section), case of Sipoş v Romania, No. 26125/04 of 3 May 2011)
  http://merlin.obs.coe.int/redirect.php?id=15260

IRIS 2011-9/1

Germany

Federal Court of Justice Rules on Media Privilege

Sebastian Schweda
Institute of European Media Law (EMR), Saarbrücken/Brussels

In the context of a final appeal of points of law, the *Bundesgerichtshof* (Federal Court of Justice – BGH) recently dealt with the scope of, and limits to, the so-called "media privilege (*Medienprivileg*), which defines the relationship between data protection and freedom of speech. In its judgment of 1 February 2011, the BGH gave media and press freedom priority over the interests claimed by the plaintiff.

The case had been brought by one of the two murderers of the actor Walter Sedlmayr who had been sentenced to life imprisonment (see also IRIS 2010-2/9). He had been released on parole in January 2008 and had complained about an article published by the defendant at its internet news portal on 12 April 2005. That article reported that the *Landgericht Augsburg* (Augsburg Regional Court) was examining the possibility of reopening the criminal proceedings and mentioned the plaintiff's full name. The plaintiff wanted to prevent this as he considered that mentioning his name had an adverse impact on his interest in being reintegrated into society. In his opinion, greater priority should be attached to that interest than to the defendant's interest in publishing the plaintiff's name. The *Landgericht Hamburg* (Hamburg Regional Court) and the *Hanseatisches Oberlandesgericht* (Hamburg Court of Appeal) allowed the claim for injunctive relief against the portal operator.

The BGH set aside the judgments in the final appeal on points of law and made it clear that the public interest in obtaining information and the defendant's right to freedom of speech outweighed the convicted person's interests in the case concerned. The lower courts it said, had not taken sufficient account of the particular circumstances involved. When all the interests were balanced

© 2011, European Audiovisual Observatory, Strasbourg (France)

against one another, it became clear that those asserted by the defendant had to be given priority: although the availability of the article constituted interference with the plaintiff's general personality right, it was not unlawful. The convicted individual's interest in becoming reintegrated into society admittedly gained in importance with the passage of time after the event but the harm done by mentioning his name was insignificant: the relevant and objective description of truthful statements about a sensational capital crime committed against a well-known actor was unlikely to "expose (the plaintiff) publicly for all time or to stigmatise him once again". Moreover, the article had been filed in the archive section of the portal and was expressly marked as an old report, so that obtaining knowledge of it presupposed a targeted search. However, the court went on, the offender had no right to complete "immunisation". A general requirement to remove all earlier descriptions of the offence identifying the perpetrator would "constrict the free flow of information and communication" and improperly limit freedom of speech and the media. Moreover, the court said, "(a) further aspect in the defendant's favour is the fact that the public not only has a legitimate interest in information on current affairs but also in the possibility of researching past events [...]. Accordingly, the media keep publications that have ceased to have topical relevance available for interested media users in order also to discharge their task of informing the public by exercising their freedom of speech and becoming involved in the democratic opinion-forming process".

With regard to the connection with data protection law, the BGH stated that the "media privilege" enshrined in section 57(1) of the *Rundfunkstaatvertrag* (Inter-State Broadcasting Agreement - RStV) was limited in a manner relevant to the instant case, as was, accordingly, the scope of the general provisions of the *Bundesdatenschutzgesetz* (Federal Data Protection Act) (see also section 41 of that Act, which transposes Article 9 of the Data Protection Directive 95/46/EC on the relationship between data protection and freedom of speech). That was because the article had – as required by the Inter-State Broadcasting Agreement – been exclusively made available for its own "journalistic-editorial [...] purposes". That precondition was met when the publication was aimed at an indeterminate group of people with the intention of expressing an opinion. Accordingly, the important factor for deciding who may invoke the media privilege is not the actual form of the publication but only the activity itself, which must be journalistic in nature. Internet portals, too, can therefore invoke this protection.

The BGH very clearly mentions the need for the media privilege, which has its origin in the constitutional guarantee of freedom of speech, in a key sentence of the judgment: "Without the gathering, processing and use of personal data, even without the consent of those concerned, it would not be possible for journalists to do their work, and the press could not discharge the tasks conferred on it in, and guaranteed by, Article(5)(1), 2nd sentence, of the Basic Law, Article 10(1), 2nd sentence, of the European Convention on Human Rights and Article 11(1) 1st sentence, of the European Union's Charter of Fundamental Rights".

- *Urteil des BGH vom 1. Februar 2011 (Az. VI ZR 345/09)* (BGH judgment of 1 February 2011 (Case no. VI ZR 345/09)) http://merlin.obs.coe.int/redirect.php?id=13138

IRIS 2011-5/12

France

Ban on Broadcasting Programme Showing a Minor in Difficult Circumstances without Obtaining Parents' Authorisation

Amélie Blocman
Légipresse

As part of its duty to protect children and young people, conferred on it by Article 15 of the Act of 30 September 1986, the *Conseil Supérieur de l'Audiovisuel* (audiovisual regulatory body – CSA)

© 2011, European Audiovisual Observatory, Strasbourg (France)

ensures not only the protection of young viewers but also the protection of minors taking part in television programmes. On 17 April 2007 it therefore adopted a deliberation on the participation of persons under the age of 18 in television programmes other than works of fiction (see IRIS 2007-6/17). This text reaffirms the need for young people to be able to express their opinions, and requires editors to obtain consent not only from the minor but also from the person exercising parental authority, to avoid dramatisation or derision in handling the young person's contribution, to ensure that filming conditions and the questions to be asked are suited to the child's age, to make sure the child's participation will not be damaging for its future, and to preserve the child's prospects of personal fulfilment. Editors must also ensure protection of the identity of minors talking about the difficult circumstances of their private lives where there is a risk of stigmatisation after the programme has been broadcast. In keeping with these principles, TF1 has undertaken, under the terms of Article 13 of its convention with the CSA, that when it is considering broadcasting the contribution of a minor facing difficult circumstances in its private life it will ensure the child's anonymity and obtain prior parental authorisation, in compliance with the provisions of the Civil Code.

However, further to TF1's showing of a report entitled *Enfants à la dérive* ("children adrift"), during which questions were put to a minor placed by the courts with a foster family, and whose identity was concealed, the CSA issued formal notice to the channel to comply with these provisions. The interview had been broadcast despite written refusal on the part of the child's mother. The channel referred the matter to the Conseil d'Etat, requesting cancellation of the formal notice, basing its claim more particularly on the argument that the decision would be contrary to Article 10 of the European Convention on Human Rights. In its decision delivered on 16 March 2011, the Conseil d'Etat stated that the ban, referred to in both Article 13 of the channel's convention and the deliberation of 17 April 2007 on broadcasting a programme including the participation of a minor facing difficult circumstances in its private life without obtaining authorisation from the person exercising parental authority, fell within the scope of the provisions of paragraph 2 of Article 10 of the European Convention on Human Rights. The fact that the minor's identity had been concealed was irrelevant. The requirement to obtain parental authorisation even if the minor's identity was concealed did not constitute a disproportionate infringement of the freedom of expression compared with the need to protect children and young people, as the Conseil d'Etat held that there were no grounds of general interest likely to justify not obtaining the authorisation of the person exercising parental authority. TF1's application was therefore rejected.

- *Conseil d'Etat (5e et 4e sous-sect.), 16 mars 2011 - TF1* (Conseil d'Etat (5th and 4th sub-sections), 16 March 2011 - TF1) http://merlin.obs.coe.int/redirect.php?id=13215

IRIS 2011-6/16

The Right of Reply

Iceland

New Media Law in Iceland

Páll Thórhallsson
Legislative Department, Prime Minister´s Office, Iceland and Reykjavik University in Media Law

On 15 April 2011 the Icelandic Parliament adopted a new media act, marking an end to a seven-year long struggle to have such an act enacted. In 2004 the President had vetoed a media law that foresaw ownership restrictions. Since then many different versions of media law bills have been presented in Parliament, but with no result until now.

© 2011, European Audiovisual Observatory, Strasbourg (France)

The Act implements the Audiovisual Media Services Directive. It includes many other important changes to the existing legal framework for the media. The Act replaces the 2000 broadcasting act, as well as the 1956 press act. It introduces an obligation for all media in Iceland to be registered with a new media authority, the Media Committee. The term “media” is defined as any medium that delivers edited content to the public on a regular basis whose main purpose is to provide media content. This includes broadcasting media, press media and certain types of electronic media, but excludes blogs and social media. [...]

The content obligations of the media are now more stringent than before, applying also for the first time to print and electronic media. Thus, it is stipulated that media service providers have to respect human rights and equality. They must be objective and accurate in news and news-related programmes. They must take care that different points of view are represented, both those of men and women.

The protection of journalistic sources of information has been strengthened and provisions on the right of reply and on liability for unlawful content are harmonised across all media.
[...]

• *Lög um fjölmiðla - Lög nr. 38 20. apríl 2011* (Media Act n. 38 of 20 April 2011)
http://merlin.obs.coe.int/redirect.php?id=13180

IRIS 2011-6/22

Ireland

Right of Reply Scheme Introduced

Damien McCallig
School of Law, National University of Ireland, Galway

The Broadcasting Authority of Ireland (BAI) on 3 May 2011 published the BAI Right of Reply Scheme. The Scheme, which came into effect from 4 May 2011, provides for the broadcast of a Right of Reply Statement, which will facilitate the correction of incorrect information which has been broadcast and which has resulted in a person’s honour or reputation being impugned. It will not be available in respect of incorrect facts that do not result in a person’s honour or reputation being impugned. The Scheme applies only to the correction of facts and does not provide for the broadcast of an alternative or contrary opinion.

The BAI was required by section 49 of the Broadcasting Act 2009 to prepare a scheme for the exercise of the right of reply. As required by section 49(3) of the Act, a Draft Right of Reply Scheme was published in January 2011 and a short period of public consultation closed on 4 February 2011.

The aim and objective of the Scheme is to offer a timely, efficient and effective mechanism that is clearly understood, proportionate and fair to all sides. Exercising a right of reply is free of charge and it offers the individual an alternative to the legal route in order to correct the broadcast of incorrect facts about him/her. Utilising the Scheme does not prevent an individual from taking legal proceedings in relation to a broadcast. However a defendant in a defamation action may seek to lessen damages by giving evidence that he/she granted or offered a right of reply.

The Scheme under section 2 details the process for exercising a right of reply. This includes the requirement that the request must be in writing to the broadcaster and that the request must usually be made not later than 21 days after the date of broadcast. Section 2 also details the potential outcomes of a right of reply request. Where a decision to refuse a request has been made, the broadcaster must inform the compliance committee of the BAI.

© 2011, European Audiovisual Observatory, Strasbourg (France)

Section 3 of the scheme describes the information a Right of Reply Statement should contain and the form the statement should take. As a general principle, a right of reply should be broadcast at a time and in a manner and with a prominence equivalent to that of the original broadcast.

A refusal of a right of reply request can be reviewed (section 4). The review request must be made in writing to the BAI Compliance Committee. A reviewable decision to refuse can also arise where a broadcaster fails to make a decision within 10 days, if the form of a right of reply statement cannot be agreed or if a broadcaster refuses to broadcast a right of reply statement formerly agreed.

Where a refusal is annulled by the compliance committee a broadcaster must broadcast the decision within 7 days of being notified. If a broadcaster fails to broadcast the decision, the compliance committee can recommend that the BAI applies to the High Court for an appropriate order to ensure that the broadcaster complies.

The Scheme applies to all broadcasters regulated in the Republic of Ireland. It does not apply to broadcasters licensed in other countries but widely received in the Republic of Ireland. Under section 49(27) of the Broadcasting Act 2009 the BAI is required to review the operation, effectiveness and impact of the Scheme no later than three years after its operation and every five years thereafter or at such a time as requested by the Minister for Communications, Energy and Natural Resources.

- Broadcasting Authority of Ireland, "BAI Right of Reply Scheme", 3 May 2011
  http://merlin.obs.coe.int/redirect.php?id=13326

IRIS 2011-7/28

Slovakia

Amendment to the Press Act

Jana Markechova
Markechova Law Offices

On 1 September 2011 Act No. 221/2011 Coll. amending and supplementing Act No. 167/2008 Coll. on periodicals and news agency services (hereinafter referred to as the "Press Act") proposed by the Minister of Culture on 15 February 2011 shall come into force (hereinafter referred to as the „Amendment").

[…]

Most importantly, it has restricted the right of reply of public officials with regard to statements concerning the performance of their functions (s. 8(2) of the Amendment). However, it is to be noted that such restriction shall not apply to statements of fact referring to a person performing the function of a public official as a private person.

In order to achieve exactness, the Amendment provides a clarification of the term "public official" and also refines the character of "a statement of fact", in relation to which persons concerned will have the right of reply, i.e., untrue, incomplete or distorting factual statements concerning the honour, dignity or privacy of a natural person or the name or good reputation of a legal entity. It is interesting to mention that according to the previous regulation any statement (i.e., either untrue or true relating to the particular natural person or legal entity) was subject to the right of reply and it was also possible for the person concerned to exercise the right of reply as well as the right of correction concurrently. However, according to the Amendment, by publishing a reply the right of correction relating to the same matter is extinguished.

© 2011, European Audiovisual Observatory, Strasbourg (France)

Other important changes introduced by the Amendment include those regarding the extent of certain obligations relating to the publication of a correction, reply and additional announcement. The Amendment introduces a wider range of grounds on which publishers of periodicals and press agencies may refuse to publish such a correction. The common ground allowing the refusal to publish a correction, reply as well as additional announcement includes the case in which the publication thereof could cause the commitment of a crime, misdemeanour or other administrative offence or be contrary to good manners or the interests of a third party protected by law.

Moreover, under the Amendment the right of monetary compensation in the case where a correction, response or additional announcement is not published or some of the conditions necessary for its publication are not met, has been abolished.

[…]

- *Zákon z 29. júna 2011, ktorým sa mení a dopĺňa záko č. 167/2008 Z. z. o periodickej tlači a agentúrnom spravodajstve a o zmene a doplnení niektorých zákonov (tlačový zákon) a ktorým sa mení zákon č. 308/2000 Z. z. o vysielaní a retransmisii a o zmene zákona č. 195/2000 Z. z. o telekomunikáciách v znení neskorších predpisov* (Act No. 221/2011 Coll. Of 29 June 2011 amending and supplementing Act No. 167/2008 Coll. on periodicals and news agency services) http://merlin.obs.coe.int/redirect.php?id=13454

IRIS 2011-8/43

Self-regulation

Spain

RTVA adopts a Self-Regulation Code on the Reporting of Sexist Violence on Television

Trinidad García Leiva
Universidad Carlos III de Madrid

The Council of Professionals of Canal Sur Television and Canal Sur 2, both Andalusian public service broadcaster Radio y Televisión de Andalucía (RTVA) channels, have elaborated a code containing recommendations and guidelines on gender equality and the portrayal of sexist violence on television. These consist of a set of principles to be followed by professionals linked to the corporation and have been developed in broad consultation with experts in law, security and sociology, as well as with associations for gender equality and protection.

By the end of June 2011 RTVA's general manager, Pablo Carrasco, was presented with a Self-Regulation Code on Sexist Violence Related Information that aims to combat sexist stereo-types and violence in the media, while backing public policy on gender equality. The document, closely connected to journalism ethics, presents best audiovisual editorial practices and answers to most frequently asked questions and doubts as regards sexism, violence and privacy issues.

A special conference dedicated to the protection of minors and the reporting of violence against women on television, held by Canal Sur in Seville, was the origin of the code, which is dedicated to supporting the use of non-sexist language in the media, especially when reporting news. The initiative is one of the first of its kind in Spain.

© 2011, European Audiovisual Observatory, Strasbourg (France)

• *Código de los Profesionales de CSTV para la elaboración de informaciones sobre violencia machista* (Code of the Professionals of Canal Sur Television on the reporting of sexist violence) http://merlin.obs.coe.int/redirect.php?id=13404

IRIS 2011-8/25

Italy

AGCOM Regulation and Self-Regulatory Rules on the Representation of Judicial Processes in Television

Manuela Branco
Autorità per le garanzie nelle comunicazioni (AGCOM)

At the beginning of 2008 Agcom (the Italian Communications Authority) adopted Deliberation no. 13/08/CSP, pointing out the risks that arise from making a show of ongoing judicial processes in TV programmes, such as docu-dramas and docu-fictions, which reconstruct legal case in spectacular and attractive ways, in order to increase the audience by creating a sort of media tribunal that almost replaces the real one and compromising objectivity and impartiality of information.

Throughout the above-mentioned deliberation, Agcom set out the following guiding principles for a correct representation of judicial processes on TV: media overexposure or artificial description of trials in progress, which make it hard for the viewer to have an appropriate comprehension of the facts, shall be avoided; on the one hand, the right to inform should not be affected, but on the other hand, the presumption of innocence of the defendant should be protected; information shall respect the principles of completeness, accuracy, fairness and protection of human dignity, avoiding turning private pain into a public show and implementing strengthened protections when minors are involved.

In addition to this deliberation, Agcom invited broadcasters, in association with the Italian order of journalists, to adopt a self-regulatory code in order to ensure the concrete implementation and enforcement of these criteria. This code was adopted in May 2009, and in addition to the transposition of Agcom's instructions into concrete rules for a proper representation of judicial processes in TV, it also provided for the establishment of a specific Committee charged with monitoring their compliance, as well as adopting measures in cases of infringement.

The Committee first met on 17 December 2009, and on the same date, the self-regulatory code came into force. On 18 July 2011, the working procedures of the Committee were adopted by the signatories of the code and then published on Agcom's website.

According to these procedures, anyone who considers a programme not to be compliant with the self-regulatory rules can report it in detail to the Committee, filling in the specific form available on Agcom's website. The Committee will screen all reports in advance, in order to verify their completeness, validity and admissibility, and, afterwards, the President of the Committee will choose a member from among Agcom's representatives as rapporteur of the investigation phase. The report will be transmitted to the broadcaster concerned, who can defend itself in writing, as well as ask for a hearing within 15 days. The Committee will also acquire the recording of the contested programme.

At the deadline, the rapporteur will inform the President of the closing of the investigation phase and email all relevant documentation to him/her. The President will then convene with the Committee, which will decide by absolute majority. Where an infringement of the Code is ascertained, the broadcaster will have to communicate it to the public within a suitable term and the deliberation will be published on Agcom's website.

© 2011, European Audiovisual Observatory, Strasbourg (France)

- *Delibera n. 13/08/CSP - Atto di indirizzo sulle corrette modalità di rappresentazione dei procedimenti giudiziari nelle trasmissioni radiotelevisive, Gazzetta Ufficiale della Repubblica italiana n. 39 del 15 febbraio 2008* (Deliberation no. 13/08/CSP - Guidelines for a correct representation of judicial processes in TV, Official Journal No. 39 of 15 February 2008)
  http://merlin.obs.coe.int/redirect.php?id=15272

- *Codice di autoregolamentazione in materia di rappresentazione di vicende giudiziarie nelle trasmissioni radiotelevisive sottoscritto 21 maggio 2009* (Self-regulation code on representation of judicial processes on TV signed on 21 May 2009)
  http://merlin.obs.coe.int/redirect.php?id=15373

- *Regolamento di procedura del Comitato di applicazione del Codice di autoregolamentazione in materia di rappresentazioni televisive di vicende giudiziarie adottato il 18 luglio 2011* (Working procedures of the Committee for the enforcement of a self-regulation code on the representation of judicial processes in TV adopted on 18 July 2011)
  http://merlin.obs.coe.int/redirect.php?id=15274

IRIS 2011-9/27

France

France Télévisions Adopts a "Channels Charter"

Amélie Blocman
Légipresse

The public-service television company France Télévisions has just adopted a "Channels Charter". Its Chairman and Managing Director, Rémy Pflimlin, claims it is the first to be drawn up by an audiovisual group in France. Public-sector television has a particular role to play in the country's democratic life as well as in its social and cultural life - on the basis of this idea, the France Télévisions group wanted to define the fundamental principles that ought to determine the course of its action and that of its employees.

The text recalls the "ethical rules" and the "public-service missions" required of the holding company's channels, including "honesty of information", "transparency", the "independence and pluralism of information", and the "representation of the diversity of the population of France". Faced with the multiplication of sources of information, particularly the Internet and the use of browsers, the charter recalls that journalists are required to check "every item of information" before presenting it on the air and to check all images that are to be broadcast: "journalists shall ensure that images broadcast correspond to the subjects they are supposed to illustrate". In order to preserve the independence of professionals working for France Télévisions, the charter provides that they must avoid "any situation that might cast doubts on the company's impartiality and its independence in relation to pressure groups of an ideological, political, economic, social or cultural nature". Employees must "take care to avoid any surreptitious advertising" and refuse "money, gifts, gratifications, travel, holidays or other favours or advantages of any kind whatsoever that might prejudice their independence and their credibility". They must also exercise caution when using blogs and social networks, ensuring "respect for professional and ethical rules", and refrain from compromising their credibility or that of the company. In this respect, the charter has been supplemented by an "employees' guide to good practices on social networks" since "all France Télévisions' employees may talk about their employer some day". The document covers a dozen points, recalling the ban both on comments that are slanderous, defamatory or racist, and the divulgence of in-house, confidential and/or financial information specific to the company. Employees are also to be held personally responsible for the content they publish in a blog or on a site, media or social network. It is also recommended that journalists should not

© 2011, European Audiovisual Observatory, Strasbourg (France)

tweet about what they did not say on screen, and that they should always indicate the source of content and always check on an item of news before communicating it. Extracts from the "Channels Charter" are expected to be incorporated in the collective agreement that is currently under negotiation.

• *Charte des antennes de France Télévisions* (Charter of the channels of France Télévisions)
http://merlin.obs.coe.int/redirect.php?id=15282

IRIS 2011-9/19

Internet Regulation and Freedom of Expression

OSCE

June 2011 Joint Declaration by the Four Special International Mandates for Protecting Freedom of Expression

Toby Mendel
Centre for Law and Democracy

On 1 June 2011 the four special IGO mandates for protecting freedom of expression, the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) and the Special Rapporteur on Freedom of Expression and Access to Information, adopted a Joint Declaration. The Declaration was adopted with the assistance of the Centre for Law and Democracy and ARTICLE 19 [...].

The 2011 Declaration builds on a significant focus on the Internet by some of the special mandates in recent years. The OSCE Representative has just launched a major survey of participating States' law and practice regarding the Internet, entitled "Freedom of Expression on the Internet". The Internet was also the main thrust of the 2011 Annual Report by the UN Rapporteur to the Human Rights Council.

The preamble to the Joint Declaration highlights both the unprecedented power of the Internet to enable realisation of freedom of expression and growing threats to freedom of the Internet. It notes the "transformative nature" of the Internet for people in countries all over the world, both in terms of giving them a voice and in enhancing access to information. But it also notes that billions of people still lack any, or at least good quality, access to the Internet. Furthermore, many States have actively sought to control Internet content, while others have, sometimes even in good faith, imposed excessive restrictions on Internet freedom. The preamble also notes that some States have sought to "deputise responsibility" for policing the Internet to the increasingly diverse range of intermediaries providing Internet services.

The main body of the Joint Declaration is divided into six sections dealing, respectively, with General Principles, Intermediary Liability, Filtering and Blocking, Criminal and Civil Liability, Network Neutrality and Access to the Internet. The first section makes the fairly obvious points that freedom of expression applies to the Internet, that regulatory systems designed for other technologies cannot simply be imposed on the Internet, that self-regulation can be an effective tool in addressing harmful speech on the Internet and that awareness-raising is important. It calls for more attention to be given to developing "alternative, tailored approaches" for the Internet. Importantly, it recognises the systemic nature of the Internet, calling for assessments of the

© 2011, European Audiovisual Observatory, Strasbourg (France)

proportionality of restrictions to take into account its overall power to "deliver positive freedom of expression outcomes". […]

- Joint Declaration on Freedom of Expression and the Internet by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 1 June 2011 http://merlin.obs.coe.int/redirect.php?id=13400

IRIS 2011-8/2

Commonwealth of Independent States

Model Law on Internet Regulation

Andrei Richter
Faculty of Journalism, Moscow State University

The Commonwealth of Independent States (CIS) Interparliamentary Assembly which is currently comprised of delegations from the parliaments of Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russian Federation, Tajikistan and Ukraine enacted on 16 May 2011 a Model Statute on the Basics of Internet Regulation (Модельный закон «Об основах регулирования Интернета»). It consists of 3 chapters with a total of 13 articles.

The Act sets out principles and determines major directions of regulation of relations that have to do with the use of Internet, sets procedures for state support of its development, and rules for determining place and time of legally relevant actions with the use of Internet.

The Model Statute (Art. 2) provides definitions of "Internet", "operator of Internet services", "national segment of Internet", etc. Article 5 sets out principles of legal regulation such as: (1) protection of human rights and liberties, "including the right to use Internet and access to the information placed there"; (2) consideration of peculiarities of construction and development of Internet, including existing international rules and technical procedures; (3) limitation of state regulation by the subject-matters that are not or may not (due to national law) be regulated by international norms or rules adopted by self-regulatory organizations of users and operators of Internet services; (4) non-proliferation of regulation of relations that are connected with the development of Internet and "do not touch upon the rights and interests of a human being, society and the state".

State bodies are required to provide conditions for the equal and non-discriminatory access to Internet of all users (Arts. 7 and 10). They shall not allow for "ungrounded" restrictions on the activity of operators of Internet services and on the exchange of information via Internet (Art. 7).

CIS member states are encouraged to oblige operators of Internet services to store data on the users and services provided to them for at least 12 months and to supply it upon request to the courts and/or law-enforcement agencies for the sake of counteraction to illegal activities with the use of Internet (Art. 13).

Article 11 of the Model Statute stipulates that legal actions with the use of Internet are considered as performed on the territory of the state if such an action that gave rise to legal consequences was committed by a person during his stay in that state. The time of such an action is the time of the first action that gave rise to legal consequences.

© 2011, European Audiovisual Observatory, Strasbourg (France)

• Модельный закон “Об основах регулирования Интернета” (Model Statute “On the Basics of Internet Regulation”, adopted at the 36th plenary meeting of the CIS Interparliamentary Assembly (Resolution No. 36-9 of 16 May 2011)) http://merlin.obs.coe.int/redirect.php?id=13446

IRIS 2011-8/10

© 2011, European Audiovisual Observatory, Strasbourg (France)

The Legal Framework for the Use of Personal Data by the Media

Sebastian Schweda,
Institute of European Media Law (EMR), Saarbrücken/Brussels

The tense relationship between freedom of expression and personality rights raises legal questions concerning the respective scope of and boundaries between these rights. These have already been discussed in a practical context in the lead article.[1] The first two parts of this edition of ZOOM explain the general legal framework which the Council of Europe and the European Union have created for their respective member states. Using the example of the German legal system, the third section illustrates legislative and co-regulatory measures that help to balance these rights.

The relationships between the media and subjects of journalistic activity, and between the media and their users, are governed by fundamental rights: on the one hand, fundamental rights guaranteeing certain freedoms to individuals serve to protect them from the state and therefore define the (broad) margins within which legal entities can, in principle, operate without state interference. On the other, however, fundamental rights are also protective rights which oblige the state to shield individuals from unlawful intrusions by third parties.[2] The framework within which fundamental and human rights must, in individual cases, be balanced out in this area is, in the European context, mainly defined by the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) of the Council of Europe and the Charter of Fundamental Rights of the European Union (CFR).[3]

The fundamental rights that protect the media are particularly set out in Article 10(1) ECHR and Article 11 CFR. The rights of individuals to protection of their personality rights and privacy are safeguarded by the restricting provisions of Article 10(2) ECHR[4] and Article 11 in conjunction with Article 52 CFR, and guaranteed by independent fundamental rights in Article 8 ECHR and Articles 7 and 8 CFR.

The scope of these rights is described below, including with reference to clarifying provisions of Council of Europe conventions, recommendations of the Committee of Ministers of the Council of Europe and EU secondary law.

1) Alexander Scheuer/Sebastian Schweda, "*Der Schutz personenbezogener Daten und die Medien*", in: European Audiovisual Observatory (ed.), Limits to the Use of Personal Data, IRIS *plus*, 2011-6, p. 7.
2) See Achim Seifert, "*Die horizontale Wirkung von Grundrechten*", EuZW 2011, p. 696 *et seq*.
3) OJEU of 14 December 2007, C 303, p. 17 *et seq*. The Official Journal of the EU and the Official Journal of the EC are available at: http://eur-lex.europa.eu
4) Restricting provisions such as those contained in Article 10(2) ECHR describe the framework within which, according to the ECHR, state measures to limit the protection provided by a fundamental right (in this case, the freedom of expression) can be justified.

© 2011, European Audiovisual Observatory, Strasbourg (France)

I. Rights of the Media

1. Human Rights, Fundamental Rights, Civil Rights

Article 10(1) ECHR stipulates the following:

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises."

The first two sentences are incorporated word for word in Article 11(1) CFR. The reference to licensing procedures for broadcasters, for example, contained in the third sentence of Article 10(1) ECHR is not found in the CFR. However, Article 11(2) CFR stresses that:

"The freedom and pluralism of the media shall be respected."

Although it is not explicitly mentioned in the text, the established case law of the European Court of Human Rights suggests that Article 10 ECHR considers freedom of the media (particularly press and broadcasters) as a particular form of the freedom of expression. The Court recognises media diversity as one of the "rights of others" that must be protected under Article 10(2) ECHR.[5] The state is considered to be the ultimate guarantor of pluralism, particularly in the audiovisual media.[6]

The right to freedom of expression is defined in more detail in the second sentence of Article 10(1) ECHR and the identical second sentence of Article 11(1) CFR, which differentiate between the freedom of opinion (i.e. the freedom to hold an opinion) and the freedom to receive and impart "information and ideas". The latter freedom is therefore divided into the freedom to receive information and the freedom to impart it. The right to receive information (so-called passive freedom of information) includes the right to solicit generally accessible information without disproportionate state interference. According to this interpretation, the state must, in general, refrain from making public confidential information, but it must ensure that people can obtain essential information. The right to impart information (so-called active freedom of information) is essentially identical to the right to freedom of expression.[7]

Even though it is not expressly mentioned, the freedom of the press is generally understood[8] to be specifically protected under Article 10(1) ECHR. Its scope of protection – which is, to that extent, independent – includes periodically printed publications, whereas one-off publications, such as books or leaflets, fall under the scope of (general) freedom of expression.[9] It covers the whole process of preparing the publication, particularly journalistic research and the publication of acquired information.[10] The protection of editorial secrecy, which is not discussed in detail in this IRIS *plus*, also falls under the freedom of the press. Both journalists and publishers are entitled to such protection.[11]

---

5) See European Court of Human Rights decision of 28 March 1990, *Groppera Radio AG et al. v. Switzerland*, no. 10890/84, para. 69 *et seq*. Regarding possible restrictions of the freedom of expression, see section II. 1, below.
6) See, for example, European Court of Human Rights decision of 24 November 1993, *Informationsverein Lentia et al. v. Austria*, no. 13914/88, para. 38, particularly with regard to audiovisual media.
7) Christoph Grabenwarter, *Europäische Menschenrechtskonvention*, 4th ed., Munich/Basel/Vienna, 2009, section 23 I 2 b, para. 5, p. 269.
8) The European Court of Human Rights has considered the scope of the freedom of the press on many occasions; see, for example, decision of 26 April 1979, *Sunday Times v. United Kingdom* (I), no. 6538/74; decision of 25 March 1985, *Barthold v. Germany*, no. 8734/79.
The Court's decisions are available at: http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en
9) *Grabenwarter, op. cit.,* section 23 I 2 c, para. 7, p. 270. The European Court of Human Rights assumes that the press is protected and stresses the particular importance of the protection of the press; see its decision of 27 March 1996, *Goodwin v. UK*, no. 17488/90, para. 39. This special protection is mainly exercised in the assessment of proportionality with regard to the particular circumstances in which an intrusion may be justified.
10) See section II of the lead article for details.
11) European Court of Human Rights, decision of 11 January 2000, *NEWS Verlags GmbH v. Austria*, no. 31457/96.

© 2011, European Audiovisual Observatory, Strasbourg (France)

The freedom of broadcasting, which is also protected under Article 10 ECHR, includes the dissemination of information and ideas by both radio and television, regardless of the type of transmission technology used. As with the freedom of the press, all activities linked to the preparation and implementation of the broadcast are protected.

Since the European Court of Human Rights ruled on the *Lingens v. Austria* case,[12] it has been established that the freedom of expression protected under Article 10(1) ECHR[13] includes both statements of fact and value judgements. However, statements of fact must be provable if they are to be protected, whereas this does not, in principle, apply to value judgements, such as the one on which the aforementioned case was based.[14]

The subjects of journalistic activity are protected by Article 8 ECHR and the parallel provisions of Articles 7 and 8 CFR on the right to respect for family and private life and to protection of personal data. The scope of this protection is discussed in section II. of this article. Here, it should just be pointed out that these fundamental rights are also not guaranteed without restriction. According to Article 8(2) ECHR, interference is particularly admissible if it is

> “in accordance with the law and is necessary in a democratic society … for the protection of the rights and freedoms of others.”

Restrictions of the fundamental rights described in the CFR must be measured against the general limitation of Article 52(1) CFR, which states that they must be

> “provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet … the need to protect the rights and freedoms of others.”

Pursuant to Articles 52(3) and 53 CFR, the level of protection provided by the ECHR cannot be reduced by the CFR. The “rights and freedoms of others”, which can justify the limitation of rights under Articles 7 and 8 CFR, are those described in the ECHR and CFR. Both the ECHR and the CFR state that limitations must be provided for by law. They must also be “necessary in a democratic society” or “necessary” and respect the principle of proportionality. Here, the European Court of Human Rights checks whether the reasons given by the national courts or authorities to justify interference with the rights protected under Article 8 in order to protect the rights and freedoms of others are “relevant and sufficient” for the purposes of Article 8(2) ECHR.[15]

As part of the passive freedom of information, Article 42 CFR provides for a “right of access to documents of the institutions, bodies, offices and agencies of the Union”, which more or less repeats Article 15(3), first subparagraph, of the Treaty on the Functioning of the European Union (TFEU). The right enshrined in Article 15 TFEU is given practical expression in Regulation (EC) No. 1049/2001 on access to EU documents.[16]

---

12) European Court of Human Rights, decision of 8 July 1986, *Lingens v. Austria*, no. 9815/02.

13) The scope of protection of Article 11 CFR is not yet the subject of such extensive case law as that of Article 10(1) ECHR. However, according to Article 6(1)(3) TEU (in the consolidated version of the Treaty of Lisbon), the rights in the CFR should be interpreted in accordance with the general provisions in Title VII of the CFR and with regard to the explanations referred to in the CFR that set out the sources of those provisions.

14) As far as justification is concerned, however, the Court takes into account whether there is a sufficient factual basis for the value judgement expressed. A value judgement which is not at all backed up by facts can be considered “excessive”; see the Court’s decision of 27 May 2001, *Jerusalem v. Austria*, no. 26958/95, para. 43; and decision of 26 April 1995, *Prager and Oberschlick v. Austria*, no. 15974/90, para. 37.
Although the Court decided the *Lingens* case solely on the basis of Article 10 ECHR, in the *Pfeifer* case (decision of 15 February 2008, *Pfeifer v. Austria*, no. 12556/03) it weighed the right to protection of privacy against the right to freedom of expression on the basis of Article 8 ECHR and ruled that Article 8 ECHR had been breached because Austria had insufficiently protected the reputation of the journalist Pfeifer.

15) See, for example, the Court’s decision of 8 July 2003, *Sahin v. Germany,* 30943/96, para. 63.

16) Regulation (EC) No. 1049/2001, see Lead Article, footnote 10.

© 2011, European Audiovisual Observatory, Strasbourg (France)

The relationship between freedom of information and the protection of privacy was particularly relevant to a recent case in which the Commission was asked, with reference to the aforementioned Regulation, to furnish the full minutes of a meeting including all names of the participants (the Commission had agreed to provide the minutes but had blanked out certain names). Following the Commission's refusal to fully disclose the document with all the names, the applicant brought an action in front of the Court of First Instance. The court upheld the complaint, basing its decision on the notion that Article 8 ECHR did not prevent access to the personal data in question.[17] The Court of Justice annulled this judgment, taking into account that any undermining of privacy and the integrity of the individual "must always be examined and assessed in conformity with the legislation of the Union concerning the protection of personal data, and in particular with Regulation No 45/2001".[18] The plaintiff had failed to sufficiently justify the need to disclose the data. The Commission had therefore been unable to examine the possibility of a derogation from the provisions of the EC Data Protection Regulation.[19]

2. Other European Law

Content is regulated in EU law, particularly in the audiovisual sector: as well as restricting certain types of advertising, the expression of opinions such as those that incite hatred, and pornographic content, the Audiovisual Media Services Directive[20] contains provisions on the right of reply (see II. 2. b), below).

The Council of Europe has adopted numerous legal instruments aimed at guaranteeing the freedom of expression, media and information. The Committee of Ministers has dealt with individual aspects of these rights in a multitude of recommendations.

Recommendation No. R(81)19 on the access to information held by public authorities[21] and Recommendation No. Rec(2002)2 on access to official documents are aimed at promoting freedom of information.[22] Exceptions to the general freedom of access to information may be made, for example, in order to protect privacy or other legitimate private interests, if they are laid down by law, necessary in a democratic society and proportionate.

Recommendation No. Rec(2003)13 on the provision of information through the media in relation to criminal proceedings deals with the rights of the media in light of the need to protect the personality rights and right to privacy of the people involved.[23] It recognises the media's right to receive information about the activities of judicial authorities and police services and particularly to report on the functioning of the criminal justice system. However, the recommendation states that the presumption of innocence must be upheld. The provision of information about suspects, accused or convicted persons or other parties to criminal proceedings should respect their right to protection of privacy. It is recommended that particular protection should be given to minors or other vulnerable persons, as well as to victims, witnesses and the families of suspects. The ministers also suggest that criminals after they have served their sentence should not be mentioned in connection with their previous offences so as to allow their identification, unless they have

---

17) Court of First Instance, T-194/04, judgment of 8 November 2007, *Bavarian Lager v. Commission*. Decisions of the EC/EU courts are available at: http://curia.europa.eu/

18) Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJEC of 12 January 2001, L 8, p. 1 *et seq*. Many of the provisions are based on Directive 95/46/EC. In addition, Articles 34 *et seq*. contain rules on the protection of personal data and privacy in the context of internal telecommunications networks operated under the control of EU institutions or bodies, which are based on the relevant standards of Directive 2002/58/EC. See II. 2. a), below.

19) Court of Justice, judgment of 29 June 2010, case C-28/08 P, *Commission v. Bavarian Lager*.

20) Directive 2010/13/EU, see Lead Article, footnote 8.

21) Recommendation of 25 November 1981 of the Committee of Ministers on the access to information held by public authorities. Council of Europe documents are available at: https://wcd.coe.int/

22) Recommendation of 21 February 2002 of the Committee of Ministers to member states on access to official documents.

23) Recommendation of 10 July 2003 of the Committee of Ministers to member states on the provision of information through the media in relation to criminal proceedings.

© 2011, European Audiovisual Observatory, Strasbourg (France)

expressly consented to the disclosure of their identity or their involvement in the offence has become of public concern again. In addition, anyone who has been the subject of incorrect or defamatory media reports should have a right of correction or reply.

Committee of Ministers recommendations are not directly binding under international law. However, they serve as a reference point for the European Court of Human Rights in its interpretation of the ECHR.[24]

II. Rights of Data Subjects

1. Fundamental Human Rights

Individuals who are the subject of data processing by the media are primarily protected by the fundamental right to privacy, which is enshrined in Article 8(1) ECHR. The provision states that:

> "Everyone has the right to respect for his private and family life, his home and his correspondence."

This provision covers several rights of the individual, which together form a comprehensive barrier against third-party interference – particularly by the state – in their private life. Protection from outside intrusion covers not only their homes, as their physical "place of retreat", but also their private and family life, which in principle can take place on either private or public property. However, an intrusion can, in certain circumstances, be easier to justify if the person concerned is acting in the public sphere.

The scope of protection is not limited to the individual's own personality and privacy, but also includes relations with other people. It also covers correspondence, i.e. any communication (regardless of the medium used) that is not addressed to the public, but to individuals. The increase in electronic data processing is bringing the concept of personal data particularly into focus in relation to the definition of the scope of protection. A central aspect of the personality right described in Article 8(1) ECHR is comprehensive protection from information relating to private life (as defined in the provision) being viewed by third parties.

In Article 8 CFR, this idea is expressed in a separate basic right to data protection, applicable in addition to the right to privacy enshrined in Article 7 CFR (which is almost identical to Article 8 ECHR):

> "1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."

These fundamental rights to protection of personal data and privacy are, in principle, also used to justify restrictions of the freedom of expression and of the media, both in the case of Article 10 ECHR and Article 11 CFR. Other personality rights, particularly the right to protection of reputation, can also justify such restrictions.

24) For example, the Court interprets the freedom of expression with explicit reference to the guidelines in Recommendation No. Rec(2003)13; see Lead Article, section II. 2. b) aa).

© 2011, European Audiovisual Observatory, Strasbourg (France)

Article 10(2) ECHR expresses this limitation as follows:

"The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, … for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence … ."

As far as Article 11 CFR is concerned, as mentioned above in relation to the restriction of fundamental rights to privacy and data protection (see I. 1., above), the general rule on limitation set out in Article 52(1) CFR and the notion that the level of protection should not be lower than that provided by the ECHR (Art. 52(3) and 53 CFR) apply.

2. Other European Law

a) Right to Privacy

Article 8 CFR describes the essential principles of the legal situation created within the EU by Directive 95/46/EC[25] (and its transposition by the member states) and safeguards them under primary law. By adopting the Directive, the EC (as it was known at the time) created a common legal framework for the processing of personal data for the first time.[26] "Processing" in the sense of the Directive means, in principle, any operation performed on such data. The definition in Article 2(b) of the Directive mentions, for example:

"collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

The most important principle of the Directive is that data processing is only admissible if the data subject has given their consent or if it is permitted by law. EU data protection law is therefore based on a fundamental ban on data processing, unless consent is obtained. Data that are processed in accordance with this rule may only be

"collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes" (Art. 6(1)(b) of the Directive).

They must also be

"adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Art. 6(1)(c) of the Directive).

Under this principle, personal data cannot later be used for purposes other than those for which they were originally collected. In order to provide transparency and legal protection for data subjects at all times, their position is secured by information obligations on the data controller (Art. 11), their own right of access and right to object (Art. 12 and 14) and remedies, liability provisions and possible sanctions (Art. 22 *et seq*.). In addition, the "controller"[27] is obliged, in principle, to notify the supervisory authority before carrying out any automatic data processing operation (Art. 18 *et seq*.). However, member states can, under certain circumstances, provide for exemptions from notification if, for example, the controller appoints a data protection official (see Art. 18(2)). If

25) Data Protection Directive; see Lead Article (section II., footnote 13).
26) "Personal data" are defined in Article 2(a) of Directive 95/46/EC as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
27) The "controller" is defined in Article 2(d) of Directive 95/46/EC as the person or body which "alone or jointly with others determines the purposes and means of the processing of personal data".

© 2011, European Audiovisual Observatory, Strasbourg (France)

data are processed "solely for journalistic purposes or the purpose of artistic or literary expression", Article 9 of the Directive allows exemptions from the data protection provisions in order to protect the freedom of expression,[28] as described in more detail in the Lead Article (see II. 1.).

New impetus for the reform of EU data protection law should be provided by a Commission proposal[29] designed to strengthen the rights of individuals as well as the internal market, and to create a coherent legal framework. The Commission has announced that it will publish draft legislation and practical proposals for non-legislative measures by the end of the year.

Alongside the "General Data Protection Directive" 95/46/EC, Directive 97/66/EC introduced specific regulations on data protection in electronic communications. This Directive was replaced by Directive 2002/58/EC, which in turn was amended by Directive 2009/136/EC. These amendments include a rule that information such as cookies may only be stored in or accessed from terminal equipment with the user's consent (Art. 5(3) of Directive 2002/58/EC).[30]

The main data protection instrument of the Council of Europe is the "European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (so-called Data Protection Convention). Adopted in 1981, the Convention sets out the principles of automatic data processing. It has clear structural and content-related similarities with the Data Protection Directive, which expressly refers to the Convention in Recital 11.[31]

The Committee of Ministers of the Council of Europe has also adopted several recommendations on personal data and the right to privacy:

Recommendation No. R (99) 5 contains guidelines on the protection of individuals with regard to the collection and processing of personal data on the Internet. The guidelines set out principles of fair privacy practice. The first part is aimed at users and the second at Internet service providers.

According to Recommendation No. CM/Rec(2007)11, users should be given information about how to exercise their rights in the "new" information and communications environment.[32] The Recommendation mentions some examples of situations and the rights involved: it refers to the right to private life and the secrecy of correspondence in relation to data processing linked to the monitoring of e-mail and Internet use, the retention of personal data and profiling by search engines and content providers, the production of user-generated content (UGC) and the consumption of potentially harmful content by children. The right of access to information plays a role in relation to filtering and blocking mechanisms as well as the listing and prioritisation of information by search engines. The Recommendation also urges the Council of Europe member states, the private sector and civil society to develop forms of cooperation so that individuals can exercise their rights, in particular the right to freedom of expression and information and the right to private life and the secrecy of correspondence.

---

28) According to Recital 37, exemptions from the measures on the security of processing (Art. 17) should not, in general, be laid down. The supervisory authority must at least be given ex-post powers.

29) European Commission, Communication of 4 November 2010 to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – a comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

30) For details, see the Lead Article (III. 2. b)).

31) The Data Protection Convention does not, however, contain an equivalent provision to Article 9 of the Directive Restrictions in favour of the media must therefore be based on Article 9(2)(b) of the Convention, which permits derogations from the provisions on quality of data, highly sensitive data and data subjects' rights to protect "the rights and freedoms of others". The Explanatory Report to the Convention mentions the freedom of the press as an example. In parallel to the efforts to reform the Directive, the Convention is also currently being revised. The results of a public consultation show that some participants who looked at the relationship between data protection and freedom of expression support the introduction of a similar provision to Article 9 of the Directive; see, for example, European Broadcasting Union (EBU), comments of 3 March 2011, in: Bureau of the Consultative Committee of the Data Protection Convention (ed.), provisional report on the consultation concerning the modernisation of Convention 108, available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_01_%20MOS6%20Results.pdf , p. 149 *et seq.*, and Centre for Socio-Legal Studies, in: *ibid.*, p. 105 *et seq.*

32) Recommendation of 26 September 2007 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment.

© 2011, European Audiovisual Observatory, Strasbourg (France)

The protection of personal data in the context of profiling was dealt with in Committee of Ministers Recommendation No. CM/Rec(2010)13. Its appendix describes principles which should particularly be respected by people, public authorities and public or private bodies which participate in and use profiling. It lays down legal and technical conditions for data processing, the rights of data subjects, sanctions and remedies, measures to guarantee data security and recommendations on the role of supervisory authorities. It is also recommended that privacy and data protection issues are taken into account already at the planning stage when designing and implementing new procedures and systems, e.g. through the use of so-called "privacy-enhancing technologies" (PET).

b) Protection of Other Personality Rights

The position of individuals vis-à-vis the press is also protected by numerous media-law provisions, such as rights to information or access to information or public events (e.g. press conferences or court hearings). In 1970, the Parliamentary Assembly of the Council of Europe (PACE) considered the need to seek a balance between freedom of expression and the right to privacy. In its Resolution 428 (1970), it proposed measures to deal with this issue, including the provision of training for journalists, the drafting of professional codes of ethics and the creation of press councils. Even then, the PACE recognised the problem of attempts to obtain information using modern technical devices such as wire-tapping equipment and hidden microphones, which recently came to the fore in the *News of the World* scandal.

The right of reply also entitles individuals to defend themselves against the publication of information concerning them. It enables subjects of reporting, at least retrospectively, to put across their version of events and to correct information concerning them (often personal data) if they were unable to prevent its publication in advance (such as through measures available under data protection law). In order to be able to exercise this right meaningfully, however, they must, in some circumstances, disclose further personal data and agree to them being collected and published.

A legal basis for the right to reply is found, *inter alia*, in the EU Audiovisual Media Services Directive.[33] In Article 28 of the Directive, member states are required to establish a right of reply "or equivalent remedies".[34] Similarly, this right is mentioned in the European Convention on Transfrontier Television. Article 8(1) of the Convention requires Council of Europe member states which are parties to the Convention to offer the right of reply or "other comparable legal or administrative remedies". In order to make it easier to exercise this right, the name of the broadcaster responsible must be identified in the programme service itself at regular intervals, according to Article 8(2) of the Convention. Anyone who wishes to use a mass communication channel via which information that invades the privacy of others can be broadcast must therefore tolerate an intrusion in his own private life.

III. National Regulations

Beneath the level of fundamental rights, there is a second tier of regulations in the EU and Council of Europe member states concerning the relationship between privacy and personality rights on the one hand and the freedom of the media and freedom of expression on the other. These help to outline media rights within the overall framework of their journalistic and editorial activities and, therefore, to create adequate protection mechanisms in order to effectively combat personality right infringements in this context.

---

33) *Op. cit.* (footnote 20). The "Minimum rules regarding the right of reply" contained in the appendix to the Council of Europe Committee of Ministers Resolution (74) 26 only make provision for such a right if inaccurate facts have been published, whereas no defence against expressions of opinion is mentioned. The Council of Europe's Convention on Transfrontier Television of 5 May 1989 does not define the types of statement that can give rise to a right of reply. The right of reply can therefore apply to the publication of both inaccurate and accurate facts.

34) Article 28 only refers to (linear) television services. However, Recital 103 suggests that online services could also be included; see the Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply, OJEU of 27 December 2006, L 378, p. 72 *et seq*.

© 2011, European Audiovisual Observatory, Strasbourg (France)

These second-tier provisions vary from one member state to another. Civil law claims to injunctions, correction, retraction or damages can protect individuals if the (future or past) publication of private information actually breaches their personality rights. There may also be provisions on the protection of name and image rights.

There are also many criminal law provisions protecting the personality rights and privacy of individuals. In Germany, for example, criminal offences are defined in order to protect a person's honour and reputation (Articles 185 *et seq*. of the *Strafgesetzbuch* (Criminal Code) – StGB). Stalking and breaches of the confidentiality of communications and of intimate privacy (e.g. the production of secret audio and/or video recordings or third-party publication of such recordings) are criminal offences (see Articles 238 and 201 *et seq*. StGB). In addition, data protection rules, despite broadly defined exemptions set out in Article 9 of the Data Protection Directive, lay down minimum standards regarding the use of collected data. Conversely, the protection of the freedom of expression and freedom of the media is also taken into account in second-tier regulations through the recognition of "legitimate interests": stalking, for example, may not actually be a criminal offence if it is not "unauthorised", but takes place for commendable journalistic reasons.[35]

In addition to or instead of second-tier regulation, a third level of measures designed to provide appropriate and balanced protection may be taken by the media themselves, possibly in combination with or based on state regulation. Such a co-regulatory model exists for the press and, since 1 January 2009, for online services (except broadcasting) in Germany with the *Freiwillige Selbstkontrolle Redaktionsdatenschutz* (voluntary self-regulation of editorial data protection) of the German *Presserat* (Press Council). Publishing companies which promise to abide by the Press Council's code of conduct (*Pressekodex*) are also obliged to respect the principles it contains on editorial data protection.[36] The Press Council takes preventive measures to ensure compliance with these principles by informing parties who are bound by them and advising editorial staff. If an infringement is committed, a complaint must be lodged with the Editorial Data Protection Complaints Committee, which, in case the complaint is upheld, can issue a notice or reprimand, or express disapproval.

The above shows that striking a reasonable balance between the (active and passive) freedom of information on the one hand and personality rights on the other represents a challenge for "legislators" at all levels. Moreover, it should not be forgotten that an important role in the balancing of interests in individual cases is played by the courts, the need for which (as described in the lead article in particular) is emphatically confirmed by the frequency with which such cases are brought before national, supranational and international courts.

35) For more detail, see Matthias Seiler, *§ 238 StGB – Analyse und Auslegung des Nachstellungstatbestandes*, 2010, available at: http://tobias-lib.uni-tuebingen.de/volltexte/2010/4592/pdf/238_neu_StGB.pdf , p. 182 *et seq*.; and Art. 193 StGB. The StGB is available in English at: http://www.gesetze-im-internet.de/englisch_stgb/index.html

36) Restrictions on the processing of personal data for research purposes are set out in paragraph 4 of the code: the use of dishonest methods to collect data is prohibited. Data collected in breach of the code must be blocked or deleted. The principles laid down in paragraph 8 particularly help to protect personality rights when data is published. The foreword states that: "The press respects the private life … the privacy of people … the right to informational self-determination and guarantees editorial data protection." Finally, paragraph 13 contains guidelines on reporting on preliminary and court proceedings. Regarding the "Editors' Code of Practice" of January 2011, on the basis of which the United Kingdom's Press Complaints Commission rules on complaints about reporting, see http://www.pcc.org.uk/cop/practice.html , particularly paragraphs 3 and 10.

© 2011, European Audiovisual Observatory, Strasbourg (France)

Information services for the audiovisual sector

It is the task of the European Audiovisual Observatory to improve transparency in the audiovisual sector in Europe. It does this by collecting, processing and publishing up-to-date information about the various industries concerned.

The Observatory has adopted a pragmatic definition of the audiovisual sector in which it works. Its principal areas of interest are film, television, video/DVD, new audiovisual media services and public policy on film and television. In these five areas, the Observatory provides information in the legal field as well as information about the markets and financing. As far as its geographical scope is concerned, the Observatory monitors, records and analyses developments in its member states. In addition, data on non-European countries is also made available when judged appropriate. The various stages involved in providing information include the systematic collection and processing of data as well as its final distribution to our users in the form of print publications, information on-line, databases and directories, and our contributions to conferences and workshops. The Observatory's work draws extensively on international and national information sources and their contributions of relevant information. The Observatory Information Network was established for this purpose. It is composed of partner organisations and institutions, professional information suppliers and selected correspondents. The Observatory's primary target groups are professionals working within the audiovisual sector: producers, distributors, exhibitors, broadcasters and other media service providers, international organisations in this field, decision-makers within the various public bodies responsible for the media, national and European legislators, journalists, researchers, lawyers, investors and consultants.

The European Audiovisual Observatory was established in December 1992 and is part of the Council of Europe thanks to its status as a "partial and enlarged agreement". Its offices are in Strasbourg, France. The Observatory's membership currently comprises 37 European States and the European Union, which is represented by the European Commission. Each member appoints one representative to its board, the Executive Council. An Executive Director heads the international Observatory team.

The Observatory's products and services are divided into four groups:

- **Publications**
- **Information on-line**
- **Databases and directories**
- **Conferences and workshops**

European Audiovisual Observatory
76 Allée de la Robertsau – F-67000 Strasbourg – France
Tel: +33 (0) 3 90 21 60 00 – Fax: +33 (0) 3 90 21 60 19
www.obs.coe.int – E-mail: obs@obs.coe.int

Legal Information Services from the European Audiovisual Observatory

Order:
- **online at http://www.obs.coe.int/about/order**
- **by email: orders-obs@coe.int**
- **by fax: +33 (0) 3 90 21 60 19**

IRIS Newsletter

Legal Observations of the European Audiovisual Observatory

Online, free of charge!

The IRIS Newsletter is a topical and reliable monthly information service covering all legal developments in Europe relating to the audiovisual sector. IRIS covers all areas of law relevant to the audiovisual sector. The main emphasis of the IRIS articles is on legal developments in the fifty or so countries that make up greater Europe. IRIS reports on media legislation in the broadest sense, as well as major developments in case law, important administrative decisions, and policy decisions which will potentially affect legislation in this field.
A free subscription and the complete IRIS newsletter are available from the IRIS website: http://merlin.obs.coe.int/newsletter.php

IRIS *plus*

A legal hot topic examined from different angles

Legal, technological or economic developments in the audiovisual sector generate immediate priority information needs for professionals. IRIS *plus* identifies these issues and provides the relevant legal background. It features a combination of a lead article, related reporting and a *Zoom* section, comprising overview tables, market data or practical information. This brand new format provides you with the knowledge to follow and join in the latest and most relevant discussions concerning the audiovisual sector.
For more information: http://www.obs.coe.int/irisplus

IRIS Merlin

Database on legal information relevant to the audiovisual sector in Europe

The IRIS Merlin database enables you to access nearly 6,000 articles reporting on legal events of relevance to the audiovisual industry. These articles describe relevant laws, decisions of various courts and administrative authorities, and policy documents from over 50 countries. They also report on legal instruments, decisions and policy documents of major European and international institutions.
Free access at: http://merlin.obs.coe.int

IRIS *Special*

Comprehensive factual information coupled with in-depth analysis

The themes chosen for our IRIS *Special* publications are all topical issues in media law, which we explore from a legal perspective. IRIS *Special* publications offer detailed surveys of relevant national legislation facilitating the comparison of the legal frameworks in different countries, they identify and analyse highly relevant issues and outline the European or international legal context that influences national legislation. IRIS *Special* publications explore their legal themes in an extremely accessible way. You don't have to be a lawyer to read them! Every edition combines a high level of practical relevance with academic rigour.
For a list of all IRIS *Specials*, see: http://www.obs.coe.int/oea_publ/iris_special/index.html

IRIS *plus* 2011-6
Limits to the Use of Personal Data
24,50 € - ISBN 978-92-871-7291-4