

Limits to the Use of Personal Data

The following article:

The Protection of Personal Data and the Media

by Alexander Scheuer and Sebastian Schweda
is an extract from the publication IRIS *plus* 2011-6
"Limits to the Use of Personal Data".

The entire publication as a printed version can be purchased
from the European Audiovisual Observatory.

For further information and order possibilities, please open hyperlinks:

IRIS *plus* series
IRIS *plus* 2011-6

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

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*

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”.

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)26⁷ 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 opinions⁸ 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/>

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 documents¹⁰ 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.

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/EC¹³ (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.

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* case¹⁷ 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>

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.

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.

e) Future development of the exemption clause

In its proposals to reform EU data protection law²⁸ the Commission did not comment on the rule contained in Article 9 DPD. However, in its statement the European Parliament²⁹ 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 retaining³¹ 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

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 public³⁷ 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 patients 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.

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 parties⁴³ 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 client⁴⁵ (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

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 werden” – 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.

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 occasions⁵³ 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 2009⁵⁴ 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>

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>

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 Berlusconi's Verwicklung in Fernsehaffäre", [derstandard.at](http://derstandard.at/1310511702569/Italien-Rechtsanwaelte-bestreiten-Berlusconi's-Verwicklung-in-Fernsehaffaere), 20 July 2011, <http://derstandard.at/1310511702569/Italien-Rechtsanwaelte-bestreiten-Berlusconi's-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=0040&fase=#sed0529.stenografico.tit0040>

63) BVerfGE 66, 116 (quoted from <http://www.servat.unibe.ch/dfr/bv066116.html>).

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 legitimization 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/EC⁶⁹ 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.

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 data⁷³). 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.

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 study⁷⁹ 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 Telemédia 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.

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.

developed so far". To redress this unacceptable state of affairs, he called for corrective legal, self-regulatory⁸⁷ 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, "Provinzgekick vor Millionen Zuschauern – Facebook entdeckt den Fußball", 18 August 2011, <http://www.sueddeutsche.de/digital/englische-pokalbegegnung-im-live-stream-facebook-sorgt-fuer-fussballtausch-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>

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 suggests⁹² 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.

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.