Chapter 5
CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES IN GERMANY

Thomas Hoeren and Anselm Rodenhausen*

5.1 Introduction

The progressive digitalisation of virtually all sectors of German society has had deep impact on the constitutional-rights system. Before describing how these developments affect the interpretation and implementation of several constitutional rights or whether those rights even have an active influence on the use of ICT, we shall briefly outline the German system of constitutional rights.

In Articles 1 to 19, the German Constitution (*Grundgesetz*, hereinafter: GG) guarantees several fundamental rights – so-called basic rights – which bind the legislature, the executive, and the judiciary as directly applicable law. Beside these federal rights, most Constitutions of the sixteen federal states of Germany contain their own basic rights. According to Article 31 GG, federal law has precedence over the law of the individual federal states; therefore, the basic rights of the federal states are of minor importance and shall be omitted in this chapter.

The main function of the basic rights warranted by the German Constitution is to protect the individual from the state[1] – that is why these basic rights are also described as *defensive rights*. One way of enforcing these individual rights is to appeal on an institutional issue to the Federal Constitutional Court [*Bundesverfassungsgericht*, BVerfG]; this is called 'Verfassungsbeschwerde'.[2] In addition to their primary function as defensive rights, a third-party effect of basic rights (horizontal effect) ('mittelbare Drittwirkung') has been constructed.[3] This means that these basic rights may also have an impact on the interpretation of private law.

---

* Prof. Dr. Thomas Hoeren is Professor in Information, Media and Business Law at the Faculty of Law, University of Münster, and Head of the Institute for Information, Telecommunications and Media Law (ITM); Mag. jur. Anselm Rodenhausen is Junior Researcher at ITM.

[1] See BVerfG 15 January 1958, *BVerfGE* 7, 198, 204.

[2] See Art. 93 para. 1 No. 4a GG.

[3] See BVerfG 11 May 1976, *BVerfGE* 42, 143, 148; BVerfG 12 November 1997, *BVerfGE* 96, 375, 398, and also Jarass 1995, p. 345, 352.

R.E. Leenes, B.J. Koops and P. De Hert (Eds.), Constitutional Rights and New Technologies

To ascertain whether a basic right has been violated involves three steps: determination of the extent of protection of the relevant basic right; identification of an encroachment; and potential justification of the encroachment.

5.2 History of digital constitutional rights and changes in the constitutional system

In spite of ICT's advances, a term like 'digital constitutional rights' has yet not been added to German legal terminology. Only a few publications deal exclusively with this specific issue. In fact, the impact of new information and communication technologies has generally been analysed in the course of broad discourses about separate basic rights. The studies of Alexander Rossnagel, et al. in the late eighties were the first to solely but comprehensively cover this topic.[4]

Examining the impact of ICT not as a whole, but in conjunction with each basic right, has continued in the new millennium. Hence, the history of interpreting basic rights with regard to ICT and the changes to the constitutional system will be shown for each basic right.[5]

5.3 Privacy-related rights

5.3.1 Privacy and data protection

Neither privacy nor data protection is explicitly mentioned in the German Constitution. Although neither is specifically codified, they are part of a fundamental right that is considered to be expressed in Article 2 paragraph 1 and also in Article 1 paragraph 1 of the German Constitution: the 'general right of personality'.[6] Article 2 paragraph 1 GG reads:

> '[e]very person shall have the right to free development of his personality insofar as he does not violate the rights of others or offends against the constitutional order or the moral law.'

This broad phrasing leaves room for interpretation and underlines the function of this basic right as a catch-all element. Due to the jurisdiction of the Federal Constitutional Court, the extent of protection of the general right of personality contains

[4] See, for example, Rossnagel, et al. 1990, p. 308, for further references.

[5] For the major changes concerning the inviolability of the home, see *below* 5.3.2.

[6] As an autonomous fundamental right, it was evolved by the Federal Court of Justice (*BGHZ* 13, 124 – *Leserbrief*) and was later adopted by the Federal Constitutional Court (*BVerfGE* 6, 32, 41 – *Elfes-Urteil*).

diverse items, such as the account of a person in public,[7] the protection of personal honour,[8] portrait rights, the right of informational self-determination,[9] the privilege against self-incrimination,[10] and also privacy.[11] The right of informational self-determination is based on the Constitution; it is also referred to as the fundamental right of data protection.[12]

Generally speaking, an act of state that restricts these rights is justified if it is has a legal basis and if it is proportional. Whether the act is proportional has to be assessed by appreciation of the values at stake. Since the development of the general right of personality, the courts and literature have always stressed the relationship of this basic right to the guarantee of human dignity in Article 1 paragraph 1 GG, which is the highest value of the German Constitution.[13] This affects the relationship of the general right of personality to other values like public security or the inviolability of the body.

Although privacy and data protection coincide in some cases of legal practice, they will be analysed separately.

Current developments concerning privacy

The right to privacy as part of the general right of personality includes matters typically considered as private because of their informational content; it also includes a spatial area in which the individual can relax and find peace.[14] The Federal Constitutional Court discerns different levels of protection: the *private sphere* and the *intimate sphere*. Only the intimate sphere is fully protected.[15]

Before describing how some new technologies actually affect the constitutional protection of privacy, we shall first give a brief overview of the most frequently discussed topics concerning privacy and ICT in Germany. Both aspects of privacy protection – matters that are private because of their content and the private spatial area – face interferences due to recent developments in different ICT areas.

---

[7] See BVerfG 8 December 1983, *BVerfGE* 63, 131, 142; BVerfG 3 June 1980, *BVerfGE* 54, 148, 155.

[8] See BVerfG 3 June 1980, *BVerfGE* 54, 208, 217; BVerfG 14 January 1998, *BVerfGE* 97, 125, 147; see also the Federal Administrative Court [BVerwG] 23 May 1989, *BVerwGE* 82, 76, 78.

[9] See BVerfG 15 December 1983, *BVerfGE* 65, 1, 43 – *Volkszählung*; BVerfG 11 June 1991, *BVerfGE* 84, 192, 194.

[10] See BVerfG 8 July 1997, *BVerfGE* 96, 171, 181; see also Starck, in Von Mangoldt, et al. 2005, Art. 2 I, ¶ 100.

[11] See BVerfG 26 April 1997, *BVerfGE* 90, 255, 260.

[12] E.g., Gurlit 2006, p. 43.

[13] See BVerfG 12 November 1997, *BVerfGE* 96, 375, 398; see also P. Kunig in Von Münch and Kunig 2000, Art. 1 I, ¶ 4.

[14] See BVerfG 15 December 1999, *BVerfGE* 101, 361, 382.

[15] See BVerfG 14 September 1989, *BVerfGE* 80, 367, 373; BVerfG 14.12.2000, *BVerfGE* 103, 21, 31.

General appreciation of privacy versus security

In 2001, when the threat of terrorist assaults became eminently visible, political discussions began in Germany on how new technologies could be used to fight these menaces. By the end of 2001, the German parliament had already adopted two anti-terrorism measures, which changed seventeen bills and transferred, *inter alia*, more authority to the German intelligence services and effected the implementation of biometric identification measures – such as facial scans and fingerprints – in passports.[16] The Anti-Terrorism Act [*Terrorismusbekämpungsgesetz*], which increased the powers of the German intelligence services, was an immediate response to the September 11 attacks. Although it was originally intended as a temporary bill until January 2007,[17] this limit was eliminated in the Supplementary Anti-Terrorism Act [*Gesetz zur Ergänzung der Bekämpfung des internationalen Terrorismus*].[18]

In the run-up to the FIFA World Cup 2006 in Germany, a number of public institutions demanded advanced measures, but these were not adopted. However, when two abortive bomb attacks on German regional trains were revealed, the discussion started again and is continuing to date.[19] Besides anti-terrorism measures, there have also been discussions, some major court decisions, and several changes in bills regarding how to use ICT – particularly surveillance technology – in the battle against organised crime.[20]

Whether such measures violate or respect the fundamental right to privacy depends on the relation between privacy and security in each particular case. As mentioned before, privacy is part of the general right of personality and is therefore related to the guarantee of human dignity in Article 1 paragraph 1 GG. The right of human dignity cannot be subjected to amendments by basic law.[21] This argument can often be heard by those opposing the security measures. Privacy is claimed to be one of the fundamental liberties of the German democratic society, and the reluctance to taking severe security measures can be ascribed to historic experiences during the Third Reich and the German Democratic Republic. On the other hand, there is also the question of the value of security, which is backed by the constitutional right to life and physical integrity in Article 2 paragraph 2 GG. This article was consciously inserted at the beginning of the Constitution again as a reaction to

[16] Those were installed in October 2005; see press release of the Federal Ministry of the Interior: <http://www.bmi.bund.de/cln_028/nn_662928/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2005/06/G8__Innen__Justizminister.html>.

[17] Entry into force 1 January 2002.

[18] Enty into force 11 January 2007.

[19] See declaration of the German Federal Secretary of the Interior, Dr. Wolfang Schäuble, <http://www.bmi.bund.de/cln_028/nn_662928/Internet/Content/Nachrichten/Pressemitteilungen/2006/08/Statement__Kofferfunde.html>; for the legislative procedure of a counterterrorism data base, see *below* n. 51 and surrounding text.

[20] See *below* 5.3.2.

[21] See Art. 79 III GG.

the experiences during the Third Reich and to demonstrate its tremendous value and importance in the system of constitutional rights.[22] The basic right expressed in Article 2 paragraph 2 GG also contains an active duty ['Leistungspflicht'] of the German State to protect life and physical integrity against illegitimate encroachments of other civil persons.[23] This means that the public authorities are obliged to take action in order to guarantee these fundamental rights.

Even after the recent discussions about terrorism and organised crime, the simple conclusion can not be drawn that either privacy or security has prevailed over the other. In fact, the Federal Constitutional Court has repealed some electronic-surveillance measures and accepted others under certain licensing requirements.[24] It is all about the proportionality of a measure in the individual case.

Video surveillance

One example of the conflict between privacy and security is video surveillance of public spaces by the police. In 2003, the Higher Administrative Court of Baden-Württemberg was the first upper court to assess the legitimacy of a pilot project in which several streets and squares in a German city centre were monitored round-the-clock by eight video cameras. Images were saved on a digital video server and deleted after 24 hours.[25] In its decision, the court struck a compromise between the advocates of such observations and privacy guardians. Video surveillance of public spaces is legitimate under strict preconditions as a precautionary measure for ensuring safety. The main condition is the objective unsafeness of the place to be monitored. This means that there must be facts that provide an informative basis to assume the place will be the site of crimes. The degree of probability of crimes being committed there should be higher than in most other places in the same city. The court took into consideration that video surveillance of public places constitutes an infringement of privacy and of the right of informational self-determination of passers-by. Only the preconditions made the measure proportional. In principle, this compromise has been accepted by the literature.[26] This meant that for a long time, an expansion of video surveillance such as occurred in London did not seem to be admissible. However, after the abortive bomb attacks, politicians have called for a more intensive observation of stations and trains.

The discussion about video surveillance of work places is closely related to this. Whether or not monitoring by the employer violates the general right of personality of the employees also depends on the proportionality.

---

[22] See BVerfG 1 August 1987, *BVerfGE* 49, 12, 53.

[23] See BVerfG 21 June 1977, *BVerfGE* 45, 187, 254; BVerfG 28 January 1992 *BVerfGE* 85, 191, 192 for the protection of life; and BverfG 14 January 1981, *BVerfGE* 56, 54, 78 for the protection of physical integrity.

[24] See BverfG 3 March 2004, *BVerfG*, NJW 2004, 999 et seq.

[25] VGH Mannheim 21 July 2003, *NVwZ* 2004 p. 498.

[26] See Ogorek 2004, p.608; see also Von Stechow and Von Foerster 2004, p. 202.

In 2004, the Federal Labour Court [*Bundesarbeitsgericht*, BAG] decided that the video surveillance of a postal distribution centre where some letters had disappeared was not proportional.[27] In this particular case, the court stated that permanent surveillance pressure can strongly affect the employees' privacy and is not in proportion to the risks of the employer.[28]

Application of GPS for criminal prosecution

Another example of the constitutional relationship between privacy and security is the application of new technologies in preliminary proceedings, i.e., during the stage prior to a criminal charge in the sense of Article 6 ECHR. In 2001, the Federal Court of Justice had to decide whether GPS data that had been recorded in the preliminary proceedings could be used as evidence in a trial against a terrorist suspect.[29] The court decided that the use of GPS data is included in the German Code of Criminal Procedure [*Strafprozessordnung*, hereinafter: StPO], but this can also involve other surveillance measures such as an 'all-around surveillance', which would be an encroachment of privacy that could not be legitimated. In the same case, the Federal Constitutional Court emphasised that the use of new technologies in preliminary proceedings can strongly affect the general right of personality – in particular when those surveillance measures are unknown to the suspect.[30] Therefore, these measures require certain procedural regulations in order to be proportional. Because of rapid technical developments, the German legislator must keep a close eye on developments and, if necessary, enact new laws to maintain a high level of privacy protection.[31]

Consideration of privacy in relation to communication-related rights

Another, completely different, aspect is the conflict between the general right of personality – including the individual's portrait rights, free speech, and the account of a person in public – and communication-related rights. The starting point for our considerations is the relation between the general right of personality and the basic rights in Article 5 GG. These are, among others, the freedom of expression, the freedom of the press, and the freedom of art. In the leading decision, the Federal Constitutional Court affirmed the high value of the general right of personality and approved the proscription of a novel that portrayed the life of a famous German actor and his role in the Third Reich.[32]

Meanwhile, the position of the communication-related basic rights is sustained by a right called 'the information interest of the citizen'. Several media-related

[27] BAG 29 June 2004, *BB* 2005 p. 102.
[28] See BAG 29 June 2004, *BB* 2005 p. 102 at p. 107; see also Wolf 2005, p. 108.
[29] BGH 24 January 2001, *BGHSt* 46, 266.
[30] BVerfG 12 April 2005, 08 *CR* 2005 p. 569 at p. 572.
[31] See again BVerfG 12 April 2005, 08 *CR* 2005 p. 569 at p. 572.
[32] BVerfG 24 February 1971, *DÖV* 1971 p. 554 – *Mephisto*.

decisions refer to this right.[33] Nevertheless, the constitutional basis for this right is very loose and is disputable. The fundamental decision made in 1973 categorised it in the freedom of reporting by means of broadcasts and films (Art. 5 para. 1 s. 2 German Constitution);[34] others see the freedom of the media or the freedom of information (Art. 5 para. 1 s. 1 German Constitution) as the constitutional setting.[35] In any case, in literature and jurisprudence, the information interest of the citizen is seen as a constitutional right or, as the case may be, a constitution-related right.

Although the relation between privacy and communication-related rights is relevant to many cases involving new technology, and new media in particular, this relation is rarely visible in specific legal provisions. In most cases, such as the violation of the right to an individual's picture on the Internet, conflicts can be solved through general constitutional and civil law (one only has to mention the decision of the European Court of Human Rights in 2004 concerning Princess Caroline, which partly contravened the prior jurisprudence of the Federal Constitutional Court and the Federal Court of Justice, and therefore caused a stir in Germany).[36] Now, we will discuss two recent problems concerning specific digital technologies.

Publishing personal information by a search engine

An example of Internet privacy protection is the legal evaluation of (meta)search-engine results. This issue may be very specific, but it clarifies how the protection of privacy and the general right of personality are also influenced by technical feasibilities.

In 2004, a German television presenter sued a meta-search engine for injunctive relief ('Unterlassungsklage', i.e., filing a complaint for having neglected to do something). When entering the name of the presenter together with 'nude' as search terms, the search engine produced several entries giving the impression that corresponding pictures were available on the Internet. The county court sustained the claim: since the entries violated the general right of personality, the operator of the search engine should adapt the system so as to avoid future encroachments by, for example, using adequate filter software.[37] In this instance, not only the hyperlink but also the 'snippet' – the text in the results lists of an Internet search – was considered a violation.[38]

However, in the appeal procedure in 2006, the upper court had a closer look at the characteristics of a meta-search engine, which only reproduces the search results of other engines. It considered that it would not be reasonable to expect the

---

[33] See BVerfG 5 June 1973, *AfP* 1973 p. 423; BVerfG 8 July 1997, *NJW* 1997 p. 2669; BVerfG 25 August 2000, *ZUM* 2001 p. 232.

[34] See again BVerfG 5 June 1973, *AfP* 1973 p. 423 – *Lebach-Urteil*.

[35] See Fechner and Popp 2006, p. 213.

[36] Gersdorf 2005, p. 221; however, see also Stürner 2005, p. 213.

[37] See LG Berlin 7 March 2005, *K&R* 2005 p. 334 at p. 335 et seq.

[38] Affirmative in this respect, Köster and Jürgens 2006.

search engine operator to check each search result for possible encroachments of the general right of personality of individuals.[39] In fact, the operator would only be liable, if he notices violating entries and neglects his duty to remove them. In this particular case, such a breach of duty was not detected.

At first, this legal practice seems to restrict the protection of the general right of personality. In fact, it is not a restriction of the basic right itself, but of the number of persons who can be held responsible for violations of this right. This case law recognised that not every member in a chain that leads to a violation has the same technical abilities to prevent further violations.

Personal information and pictures in computer games

The plot of computer games is not always entirely fictional; some of them use as models events and persons from real life, for instance, in sport simulations. The use of the name or prominent physical features of real-life persons can violate their general personality right. It is doubtful whether in such a case, the evaluation is the same as in cases concerning films or books. Unlike publishing companies and film studios, the computer games industry cannot rely on the constitutional rights in Article 5 paragraph 1 GG.[40] It is even more difficult to say whether computer games are protected by the freedom of art (Art. 5 para. 3 GG). In the first decision of a county court on this issue, LG Hamburg argued that because of its creative elements, a computer game could be partly protected under Article 5 paragraph 3 GG.[41] However, the higher court in this case decided that the consent of the person at issue – in this case, the German National Soccer Team's goalkeeper – is needed to use his name, even if the game is considered as art.[42] Designing a virtual character who imitates a prominent sportsman is not driven by artistic intentions, but by the exploitation of the celebrity of the portrayed person. Therefore, the only basic rights that could justify an encroachment of the general right of personality are the freedom of occupation (Art. 12 para. 1 GG) and the guarantee of property (Art. 14 para. 1 GG).[43]

Current developments concerning data protection

The right of informational self-determination protects the individual against unbounded inquiry, storage, utilisation, and transmission of his personal data.[44] As in other legal systems, in Germany, data protection is also provided and implemented

[39] See KG 20 March 2006, *MMR* 2006 p. 393 at p. 394; see also Stenzel 2006.

[40] See Zagouras and Körber 2006, pp. 680, 681; however, see also Lober and Weber 2003, holding a different view.

[41] See LG Hamburg 25 April 2003, *ZUM* 2003, 689 – Oliver Kahn/Electronic Arts.

[42] Cf., Ernst 2004, p. 227.

[43] See OLG Hamburg 13 January 2004, *ZUM* 2004 p. 309 at p. 310.

[44] See BVerfG 15 December 1983, *BVerfGE* 65, 1, 42; BVerfG 17 July 1984, *BVerfGE* 67, 100, 143; BVerfG 9 March 1988, *BVerfGE* 78, 77, 84; BVerfG 14 December 2000, *BVerfGE* 103, 21, 33.

by a number of non-constitutional laws. Mostly, the Federal Data Protection Act [*Bundesdatenschutzgesetz*, BDSG] applies, which regulates the general data responsibilities of the federal authorities and private individuals. Special rules concerning new technologies can be found in, for instance, the Telecommunications Act [*Telekommunikationsgesetz*, TKG], the Telecommunications Interceptions Ordinance [*Telekommunikationsüberwachungsverordnung*, TKÜV], and the Teleservices Data Protection Act [*Teledienstedatenschutzgesetz*, TDDSG]. One of the most important changes in legislation was the implementation in 2004 of Articles 91-107 TKG, which contain rules about data transfer and reporting requirements of telecommunication providers.[45]

In principle, the basic right of informational self-determination is of significance for the interpretation of all of these laws. We go into two issues concerning new technology to show the constitutional data protection in detail. During a Data Protection Symposium in Cologne in 2005, the Federal Data Protection Commissioner gave an overview of more cases under discussion in Germany, such as an automatic emergency call system for motor vehicles, an electronic health card, and the collection of data for motorway toll levying.[46] These examples, along with the subjects addressed below, illustrate that due to the quantity of data-protection provisions in Germany, most implementations of new information technologies are discussed in the context of data protection. Therefore, surveying the discussions regarding data protection provides indications which technologies may also have an impact on other constitutional rights.

RFID

The right of informational self-determination includes the right of each individual to withhold the publication of personal facts.[47] Accordingly, the use of RFID technology, for example in passports, membership cards, or merchandise, could encroach upon this right. This is why public authorities need an Act of Parliament as a basis to authorise the use and analysis of RFID data. Such an Act would limit RFID's vast technical opportunities, in order to ensure constitutional proportionality.[48] At any rate, it is unconstitutional to generate a complete personality profile.[49]

In the business-customer relation, the consumer-goods industry does not require a basis of authorisation to use RFID in products. This means that, in contrast to public authorities, companies do not need a law that expressly empowers them to use RFID. However, the use of this technology by companies is limited by the

[45] Before 2004 those duties were part of the Telecommunications Data Protection Ordinance.
[46] See Schaar 2006.
[47] See BVerfG 15 December 1983, 08 *NJW* (1984) p. 419.
[48] See Eisenberg, et al. 2005, pp. 9-10.
[49] See BVerfG 3 March 2004, 14 *NJW* (2004) p. 999 at p. 1004 and BVerfG 15 December 1983, *BVerfGE* 65, 1, 53.

Federal Data Protection Act. Up to now, it seems that this law covers all possible applications of RFID.[50]

Digital counterterrorism data base

In September 2006, the federal states of Germany agreed on a draft law for implementing a counterterrorism data base, which had been under discussion since 2001 and which is seen as another immediate result of the September 11 attacks. This data base would contain information on terrorism suspects' religion and their travel abroad. Under certain circumstances, these data would be available to the police and the intelligence services, as well as to the Customs Criminological Office. In spite of this having been discussed for almost five years, the measure is still very controversial – most notably concerning the constitutional right of informational self-determination. Several opposition parties consider the draft unconstitutional.[51] Meanwhile, the Federal Government has voted on the draft law.[52] The current draft bill seems to be a combination of two models: on the one hand, inserting full texts in the data base, and, on the other, inserting only an index in the data base. Each version is supported by one of the two parliamentary parties in the present majority coalition.[53] This combination of models is both a political compromise and an attempt to ensure that the planned measures are proportional under constitutional law. Further developments are yet to be observed. However, regarding the relation of the right of informational self-determination to security and the proportionality of preventative measures, we refer to a decision of the Federal Constitutional Court of July 2005.[54] In this verdict, the Court set out patterns to determine when measures of prevention and preparatory prosecution measures ['Vorfeldmaßnahmen'] are proportional. According to these, an important criterion is the precise and well-defined wording of the law that authorises such measures. The more important a fundamental right is that the measures infringe upon, the more precise the laws have to be.

5.3.2 Inviolability of the home

According to Article 13 paragraph 1 GG, the home is inviolable. The intention of this basic law is to secure a spatial sphere in which the individual can develop his private life.[55] This description of its aim shows the affinity of this basic right to

[50] See Holznagel and Bonnekoh 2006.

[51] See <http://www.linksfraktion.de/pressemitteilung.php?artikel=1226929225 and http://fdp-fraktion.de/webcom/show_article.php/_c-334/_nr-486/_p-1/i.html>.

[52] See <http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2006/09/Antiterrordatei.html>.

[53] See <http://www.heise.de/newsticker/meldung/print/77693>.

[54] BVerfG 27 July 2005, *DVBl* (2005) pp. 1192 et seq. – *Telekommunikationsgesetz Niedersachsen*.

[55] See BVerfG 26 May 1993, *BVerfGE* 89, 1, 12.

privacy; as such
personality.

Yet the exter
ment and attic),
and offices.[56]
croachment on t
may be authoris
designated by l
scribed.

Therefore, th
tion. Because of
paragraph 1 GC
This may pose p
observation, for

Electronic eave

The introductio
bugs, and simil
concerning the
ing organised c
13 GG to pave
Procedure. The
Article 13 para
electronic eaves
covering the m
tional Court de
of Criminal Pro
ality because th
the relevant con
in Article 1 pa
within which p
hitherto existin
sonality:[58] not
is inviolable.[59]
gies to observe
eavesdropping

[56] See Jarass,

[57] See BVerfG

[58] See *above*

[59] For the furt
sion, see also Gus

privacy; as such, Article 13 GG is a *lex specialis* in relation to the general right of personality.

Yet the extent of protection does not only cover houses, flats (including basement and attic), hotel rooms, and sleeper cabins, but also workrooms, service rooms, and offices.[56] Article 13 paragraphs 2-7 GG contains explicit rules when an encroachment on the right is justified; paragraph 2, for instance, stipulates that searches may be authorised only by a judge or, when speed is essential, by other authorities designated by law, and that they are carried out only in the manner therein prescribed.

Therefore, this basic right is said to be the most detailed in the German Constitution. Because of this, ICT measures encroaching on the rights granted by Article 13 paragraph 1 GG have to fulfill the requirements of the codified exceptions exactly. This may pose problems when new technologies emerge that provide new modes of observation, for example, electronic eavesdropping.

Electronic eavesdropping

The introduction of competences for the prosecution authorities to use wiretaps, bugs, and similar equipment in the domicile of suspects was similar to the cases concerning the general right of personality. The measures should be used for fighting organised crime. In 1998, the German Parliament had already changed Article 13 GG to pave the way for adopting these competences in the Code of Criminal Procedure. The change was necessary because the limits to the fundamental right of Article 13 paragraph 1, as stated in paragraphs 1 to 7, are very strict and exact. As electronic eavesdropping did not match one of the existing limits, new paragraphs covering the measures had to be set up in Article 13. In 2004, the Federal Constitutional Court decided that implementing acoustic domicile surveillance in the Code of Criminal Procedure, in its form at that time violated the general right of personality because the surveillance did not exclude an inner circle, which is the 'core of the relevant constitutional right' [*Kernbereich*]. The inviolability of human dignity in Article 1 paragraph 1 GG demands the absolute protection of the inner circle within which private life is arranged.[57] This decision can be seen as modifying the hitherto existing system of different levels of protection of the general right of personality:[58] not only the intimate sphere, but also a certain part of the private sphere is inviolable.[59] This means that a clause enabling authorities to use new technologies to observe citizens – like the one in the StPO that implemented electronic eavesdropping – is only in agreement with the German Constitution if it does not

[56] See Jarass, in Jarass and Pieroth 2004, Art. 13 ¶ 2.

[57] See BVerfG 3 March 2004, 14 *NJW* (2004) p. 999 at pp. 1003 et seq.

[58] See *above* n. 6.

[59] For the further development of the dogmatics of the fundamental right to privacy by this decision, see also Gusy 2004.

touch upon the inner circle of privacy. Those clauses must contain regulations to immediately stop recording if the observed individual begins a private activity, such as a personal conversation with a family member, a soliloquy, or sexual intercourse. Furthermore, there must be regulations to ensure that if such data are recorded, they may not on any account be used and have to be deleted.[60] Critics of this prominent decision by the Federal Constitutional Court have noted that a clause that meets these demands cannot be practically implemented in criminal procedure.

Meanwhile, the clause concerned has been changed. Following the new Article 100c paragraph 4 StPO,[61] electronic eavesdropping may only be implemented if there are specific indications regarding the premises to be observed as well as the relationship between the persons to be observed, and any utterances made within the person's most private sphere will not be subject to surveillance. Conversations within offices or other places of work will generally not be seen as part of a person's most private sphere. This is also valid for any conversations regarding criminal offences or any utterances by which criminal offences may be committed.

This new legislation has, again, met with some criticism. Some hold that even in its new version, the law violates constitutional rights.[62] In August 2005, the Federal Court of Justice [*Bundesgerichtshof*, BGH] decided on the first case affected by the new clause.[63] A soliloquy of a patient in his sickroom was considered part of the totally protected inner circle of the basic rights of the inviolability of the home in connection with the general right of personality.[64] As a result, the recorded data could not be used as evidence in a criminal proceeding.[65]

The proceedings about the introduction of electronic eavesdropping discussed above also raised questions about the actual subject of the 'inviolability of the home' in a modern information society. This question seems all the more important as stone walls are no longer an obstacle to new observation technologies. By referring to human dignity and the general right of personality, the Federal Constitutional Court indicates that the 'inviolability of the home' does not aim to protect liberty or property, but privacy.

5.3.3 Inviolability of the body

Article 2 paragraph 2 GG underlines the importance of this fundamental right. It reads:

> '[e]very person shall have the right to life and to physical integrity. The freedom of the person is inviolable. These rights may be interfered with only pursuant to a law.'

---

[60] See BVerfG 3 March 2004, 14 *NJW* (2004) p. 999 at p. 1005 et seq.

[61] As amended on 24 June 2005.

[62] See Leutheusser-Schnarrenberger 2005.

[63] Based on the prior version of Art. 100c para. 4 StPO, but considering the decision of the Federal Constitutional Court.

[64] See BGH, 45 *NJW* (2005) p. 3295 at p. 3296 et seq.

[65] Id., p. 3295 at p. 3298 et seq.

In the following, we will concentrate on the developments of the right to life and the right to physical integrity.

Article 2 paragraph 2 GG has not been as closely examined in relation to the influence of ICT as other articles of the Constitution. We will therefore review a typical ICT issue, using new technology for searching the body, but we will also give some attention to biotechnology. Biomedical sciences are becoming increasingly important in this context; for instance, deciphering the human genome would not have been possible without the accelerated progress of ICT. This is why we will also consider the main discussions concerning biotechnology with respect to Article 2 paragraph 2 GG.

New technology for searching the body

There has not been an extensive discussion in Germany whether measures like face recognition or terahertz cameras violate the right to physical integrity. The main focus of the discussion on these measures is their compatibility with the general right of personality and the right of informational self-determination.

Nevertheless, the basic principles of the right to physical integrity can, of course, be applied to such technologies. Physical integrity in terms of Article 2 paragraph 2 GG is the absence of pain, of infertility, and of deformation as well as of physical injuries.[66] Measures neutral to health, like taking a blood sample, as well as measures related to medical treatment, such as medical X-ray scans, are considered encroachments of the right to physical integrity.[67] Whether or not such an encroachment is justified depends again on an evaluation of rights and the proportionality in the concrete case.

A similar evaluation is required to determine the legitimacy of new identification measures with regard to the basic right to physical integrity. Again, there has not been a great deal of discussion in Germany so far, but this may change. After the successful implementation in November 2005 of electronic passports (ePass) with a chip containing a digital photograph, as of March 2007, these chips will also include digital fingerprints.[68] Moreover, the Federal Government has plans to introduce an electronic card for foreigners [*Elektronische Ausländerkarte*], which will contain similar data and biometric signatures as the ePass, and which will act as a digital residence permit.[69]

---

[66] See BVerfG 17 January 1957, *BVerfGE* 6, 55; BVerfG 10 February 1960, *BVerfGE* 10, 322.

[67] See Hoffmann, in Schmidt-Bleibtreu, et al. 2004, Art. 2 ¶ 62.

[68] See the announcement by the Federal Ministry of the Interior on <http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Themen/Informationsgesellschaft/DatenundFakten/Biometrie.html>.

[69] This was recently announced by State Secretary August Hanning on 29 September 2006; see <http://www.heise.de/newsticker/meldung/78841/>.

Biomedical sciences and biotechnology

The latest developments in biomedical sciences, like the decoding of the human genome or pre-implementation diagnostics, do not only affect the guarantee of human dignity in Article 1 paragraph 1 GG, but also the right to life and the right to physical integrity.[70] According to the prevailing opinion, the constitutional protection of life covers unborn life – starting with the nidation of the embryo.[71] Nidation is the implantation or 'nesting' of the early embryo in the uterus. With regard to the use of biotechnology, an important question is whether prenatal life is considered to be protected at the same level as postnatal life. Some constitutional lawyers argue that the full amount of protection is given only after birth, and they plead for protection to be divided into levels, in which the intensity of protection should rise progressively with the growth of the embryo.[72] Others argue that the Parliamentary Council that drafted the German Constitution did not take progressive extension of protection into consideration.[73]

Reproductive medication and pre-implementation diagnostics have given rise to special problems. To what extent do those technologies conform to Article 2 paragraph 2 GG? One part of the German jurisprudence wants to apply the same graded levels of protection used in the legal provisions regarding abortion.[74] However, the prevailing opinion probably distinguishes between *in vivo* and *in vitro* fertilisation: the protection of life *in vitro* would be even stronger, because in default of a physical connection to the womb, the constitutional right of self-determination of the mother cannot be regarded in the evaluation of rights.

Both pre-implementation diagnostics and reproductive medicine are prohibited, with criminal sanctions, by the Embryo Protection Act [*Embryonenschutzgesetz*].[75] This high standard of protection can be regarded as a result of the impact of Article 1 paragraph 1 GG (human dignity), which also protects the embryo. Also, reproductive cloning is considered strictly unconstitutional.[76]

5.4 COMMUNICATION-RELATED RIGHTS

5.4.1 Secrecy of communications

The secrecy of communication has a constitutional source in Article 10 paragraph 1 GG, which reads:

---

[70] See Hoffmann, in Schmidt-Bleibtreu, et al. 2004, Art. 2 ¶ 61.

[71] See BVerfG 28 May 1993, *NJW* (1993) p. 1751 at p. 1753; see also D. Lorenz, in Isensee 2004, Bd. 6, § 128 ¶ 12.

[72] See Dreier 2002, p. 377.

[73] See Roth-Stielow 2002, p. 530.

[74] See Art. 218 et seq. German Criminal Code [*Strafgesetzbuch*]. See also Spranger 2003, p. 71.

[75] Embryonenschutzgesetz, last amended by Art. 22 of the Law of 23 October 2001.

[76] See Frommel 2002, p. 530.

'[t]he privacy of correspondence, posts and telecommunications shall be inviolable.'

According to paragraph 2, restrictions may be made only pursuant to law. If the restriction serves to protect the free democratic basic order ['freiheitliche demokratische Grundordnung'] or the existence or the security of the Federation or of a Federal State, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature. Though the wording may suggest that this article contains several basic rights, the courts and legal scholars agree that Article 10 paragraph 1 GG covers one collective basic right. It is the right to confidentiality of individual communications, which – due to spatial distance – is dependent on a third party for transmission.[77] Thus, Article 10 paragraph 1 GG also protects the right of privacy, but it is a *lex specialis* in relation to the general right of personality.

In terms of Article 10 paragraph 1 GG, telecommunication is defined as any individual non-material transmission of information.[78] Only acts of individual communication are covered, not acts of mass communication like television or radio. The fundamental right in Article 10 paragraph 1 GG is not linked to a specific communication technology. Each electromagnetic and other immaterial forms of transmission are covered by the extent of protection, no matter if they are analogue or digital.[79] The scope of this constitutional right is dynamic, and so, new media are automatically included.[80]

This is unproblematic and without controversy as long as the new technology is a medium of individual communications, such as e-mail. The question whether a technology like the Internet at large, which is used for individual as well as for mass communications, is protected by Article 10 paragraph 1 GG has been discussed in greater detail. This discussion refers to the cumulative integration of networks and media services described as convergence, which may gradually implicate a merging of individual and mass communications.

Some argue that the extent of protection covers each medium as far as the technical method of transmission enables individual communications, no matter if the medium is also used for mass communications. Otherwise, one would have to differentiate according to the content of communication, and this would contradict the main intent of Article 10 GG, because one could only decide whether an act of communication is protected by this basic right *after* the content has been revealed and thus the right at issue has already been encroached.[81] In this view, the Internet as a whole would be protected by Article 10 paragraph 1 GG.

---

[77] See BVerfG 9 October 2002, 14 BVerfGE 106, p. 28 et seq. at p. 36.
[78] See Jarass, in Jarass and Pieroth 2004, Art. 10 ¶ 5.
[79] BVerfGE 106, 28, 36; see also C. Gusy, in Von Mangoldt, et al. 2005, Art. 10 ¶ 40.
[80] See Löwer, in Von Münch and Kunig 2000, Art. 10 ¶ 18.
[81] See Hermes, in Dreier and Bauer 2004, Art. 10 ¶ 35.

Others claim that such an extension of the extent of protection is only necessary when – due to digitisation – it is no longer possible to technically differentiate between individual and mass communications. However, such a differentiation is still feasible if the diverse media services are based on different transmission channels,[82] like broadband. In that case, protection under Article 10 paragraph 1 GG would cover only certain services of individual communication that use the Internet for transmission – like e-mail or VoIP – but not the Internet as such.

It is undisputed that Article 10 GG also protects the possibility of communicating without revealing one's identity.[83] Both the content of communications and the attendant circumstances – such as the time and the method of communication – are protected.[84] This holds for any new communication technology. For new technologies, however, specific problems may arise in determining when a communication starts and when it ends. This can be illustrated best with the legal practice concerning mobile phones, which we discuss below.

There is also a discussion in the literature whether and to what extent there is a more general right to anonymity.[85] However, the constitutional source discussed for such a right is not Article 10 GG or any other communication-related right, but the right of informational self-determination (Art. 2 para. 1 in conjunction with Art. 1 para. 1 GG). Therefore, the 'right to anonymity' – this term is hardly ever used – is seen as a specific part of data protection.

Requesting information from mobile radio providers

In 2000, an Administrative Court had to decide whether the request for data concerning an owner of a mobile phone was an encroachment of Article 10 paragraph 1 GG. The police authorities wanted to locate the owner's position using this information because they had lost his position and he was suicidal. The responsible authorities asked the missing person's telecommunications provider to pinpoint his location using the stand-by mode of this individual's mobile phone. To determine whether such a request requires an Act of Parliament as a legal basis, it had to be clarified when exactly the protection of Article 10 paragraph 1 GG begins. The court stated that the identification of the radio cell where the mobile phone is located is the result of an act of communication that has already started.[86] As a reason for expansion in time of the extent of protection, the court argued that the owner of a mobile phone is prepared for receiving certain messages or for phone calls in general. If he had to keep in mind that even the preparation for a communication act

[82] See Löwer, in Von Münch and Kunig 2000, Art. 10 ¶ 18
[83] See Hoffmann, in Schmidt-Bleibtreu, et al. 2004, Art. 10 ¶ 9.
[84] See H. Jarass, in Jarass and Pieroth 2004, Art. 10 ¶ 9.
[85] See Bäumler 2003, p. 160, as well as Klewitz-Hommelsen 2003, p. 159.
[86] See VG Darmstadt, *NJW* 2001, 2273, 2274.

– i.e., taking his mobile phone in stand-by mode with him – could be used to locate his position, the freedom of communication would be diminished. In principle, this opinion was shared by some other courts and even the Federal Court of Justice.[87]

However, in August 2006, the Federal Constitutional Court decided that positioning a mobile phone via an IMSI catcher (a pseudo-network cell used to intercept identifying numbers of mobile phones in the vicinity) is not an encroachment of Article 10 paragraph 1 GG.[88] When using an IMSI catcher to locate the current radio cell of a mobile phone, only machines are communicating, and no exchange of information is made by humans, nor references to the content of communications are made. The mere fact of the technical function of a device as a communication medium and the emission of the device in its stand-by mode would not be considered as acts of communication in themselves, but only as the pre-condition of an act of communication. Moreover, it is true that the use of an IMSI catcher is an encroachment on the personal freedoms of Article 2 paragraph 1 GG, but whether such a measure is an unjustified infringement is mainly a question of proportionality. This depends on the individual case.

Another case, illustrating where the protection of Article 10 paragraph 1 GG ends, was also decided in 2006 by the Federal Constitutional Court. Public-prosecution authorities had confiscated an individual's mobile phone from their flat in order to view the SMS messages on that phone. According to this individual, this violated the right to secrecy of communication, among other fundamental rights. However, the court stated that when the transmission of data to the mobile phone has ended, this transmission is no longer protected by Article 10 paragraph 1 GG but by the right of informational self-determination, and possibly by the inviolability of the home.[89] The main argument of the court was that when the process of data transmission has been completed, the data that are saved on the end device are no longer threatened by the same specific risks typical for using telecommunications.

In conclusion, the actual object of protection of Article 10 paragraph 1 GG can be identified as the channel that is used for individual communication.

5.4.2 Freedom of expression

Among other communication-related constitutional rights, the freedom of expression is guaranteed by Article 5 GG. Article 5 paragraph 1 reads:

> '[e]very person shall have the right freely to express and disseminate their opinions in speech, writing, and pictures and to gather information themselves without hindrance from freely accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship.'

---

[87] See BGH, *NJW* 2003, 2034, 2035, and BGH, *NJW* 2001, 1587.

[88] See BVerfG 22 August 2006, available at <http://www.bverfg.de/entscheidungen/rk20060822_2bvr134503.html>.

[89] See BVerfG, *NJW* 2006, 976, 979.

According to paragraph 2, these rights are limited by the provisions of general laws, provisions for the protection of young persons, and by the right to personal honour. The freedom of expression is considered one of the most important fundamental rights;[90] it is said to be constitutive for a liberal democratic community.[91]

A recently discussed issue is the impact of Article 5 GG on the civil and criminal liability for hyperlinks. In April 2006, OLG Stuttgart had to decide whether Alvar Freude, a self-appointed multimedia artist, had committed a crime according to Article 86 of the German Criminal Code [*Strafgesetzbuch*], by distributing propaganda of unconstitutional organisations. The artist's web site contained several links to pages of right-wing extremists displaying national-socialist symbols and texts. His own web page also showed a documentary about freedom of speech, some statements against racism, and an appeal for an objective discussion with right-wing extremism. It was undisputed that the content of the extremist pages was liable to prosecution. However, Alvar Freude referred to the freedom of speech and the constitutional right to freedom of art. The court judged that Alvar Freude had used the content of the linked web sites with the purpose to facilitate forming an opinion.[92] In this case, the hyperlinks were therefore protected by the freedom of expression, and the court acquitted the artist. This judgment shows how the constitutional right to freedom of speech has adapted to the different ways of expressing an opinion on new media like the Internet.

5.4.3 Freedom of assembly

Article 8 paragraph 1 GG states that all Germans shall have the right to assemble peacefully and unarmed without prior notification or permission. This basic right contributes to the development of citizens' personality as well as to political decision-making.[93]

Recently, the question has been raised whether on-line demonstrations are protected by Article 8 paragraph 1 or by any other basic right. The term 'on-line demonstration' (also known as 'virtual sit-ins') describes the co-ordinated, simultaneous request of data from a certain web site by a large number of Internet users, with the intent to shut down the server of that site. Unlike DDoS attacks (distributed denial-of-services attacks), the initiators of an on-line demonstration do not use other people's computers without their consent, but they start a public appeal to other Internet users to join the 'demonstration'. In 2005, a local court stated that such an on-line demonstration is not protected by the freedom of assembly.[94] Although the relevant on-line activity was declared to the City Department of Public Order, the

[90] See *BVerfGE* 62, 230, 247.
[91] See *BVerfGE* 82, 272, 281.
[92] See OLG Stuttgart, *MMR* 2006, 387, 390.
[93] See *BVerfGE* 69, 315, 344.
[94] AG Frankfurt 22 July 2005, unpublished.

gathering of electronic signals caused by several humans to one server was not considered comparable to a real gathering of several people in one physical place. The judgment was annulled by the appellate court, but for other reasons than the applicability of Article 8 paragraph 1 GG.[95] The question whether or not such online demonstrations are protected by the freedom of assembly or the freedom of expression therefore remains unanswered.[96]

5.5 Conclusion

As we have shown, the wording of most privacy and communication-related basic rights of the German Constitution can be interpreted broadly. This facilitates an interpretation of the basic rights in order to incorporate new information and communication technologies. In particular, Article 2 paragraph 1 GG offers a flexible instrument to protect the individual from the application of new technologies by the state. As a result, there has been no need for major changes of the constitution with regard to the impact of new technologies on fundamental rights protected by Article 2 paragraph 1 GG – such as liberty, the general right of personality, and the right of informational self-determination. The open wording of this article enables the courts to embrace new technologies, an option which is repeatedly exercised by the Federal Constitutional Court. Less flexible than the comprehensive element of Article 2 paragraph 1 GG are the special basic rights of Article 5 paragraphs 1 and 3 (including the freedom of expression and the freedom of art), Article 13 paragraph 1 (inviolability of the home), and Article 10 paragraph 1 GG (secrecy of communication). A reason for this relative rigidity is that these rights provide a higher level of protection. In fact, the extent of protection of Article 13 paragraph 1 GG – due to its closely-formulated restrictions in paragraphs 2 to 7 – is high and is still interpreted broadly. However, Article 10 paragraph 1 GG will probably only protect direct acts of communication. Therefore, Article 2 paragraph 1 GG and the general right of personality have an important back-up function.

This system of special basic rights ['spezielle Freiheitsrechte'] and a catch-all basic right ['allgemeines Freiheitsrecht'] enables a comprehensive and at the same time flexible approach to new information and communication technologies. Thus, there is no need for adapting the basic rights themselves. Any changes to the fundamental rights might even restrict their application regarding the further development of ICT, because they might be limited to current technology.

However, this does not imply that no action has to be taken by the legislator. The Federal Constitutional Court has declared that due to the fast process of technical development, the German legislator needs to be very attentive and must pass new (non-constitutional) laws swiftly when needed, in order to maintain a high standard

[95] OLG Frankfurt, *MMR* 2006, 547.
[96] See also Welp 2006.

of fundamental-rights protection.[97] We fully agree with the court's statement. It is important to keep a close watch on developments in ICT and to react promptly with appropriate legal measures.

REFERENCES

BÄUMLER 2003
H. Bäumler, 'Gibt es ein Recht auf Anonymität? Macht Anonymität heute noch Sinn?', *DuD* (2003), p. 160.

DREIER 2002
H. Dreier, 'Stufungen des vorgeburtlichen Lebensschutzes', *ZRP* (2002), pp. 377-383.

DREIER AND BAUER 2004
H. Dreier and H. Bauer, *Grundgesetz – Kommentar, Band I* [Commentary of the Constitutional Law of the Federal Republic of Germany, Vol. 1] (Tübingen, Mohr Siebeck 2004).

EISENBERG, ET AL. 2005
U. Eisenberg, et al., 'Überwachung mittels RFID-Technologie', *ZRP* (2005), pp. 9-12.

ERNST 2004
S. Ernst, 'Zum Namensschutz bekannter Sportler bei Einsatz des Prominenten in einem Computerspiel', *CR* (2004), pp. 227-228.

FECHNER AND POPP 2006
F. Fechner and S. Popp, 'Informationsinteresse der Allgemeinheit', *AfP* (2006), pp. 213-216.

FROMMEL 2002
M. Frommel, 'Stufungen des vorgeburtlichen Lebensschutzes', *ZRP* (2002), pp. 530-531.

GERSDORF 2005
H. Gersdorf, 'Caroline-Urteil des EGMR: Bedrohung der nationalen Medienordnung', *AfP* (2005), pp. 221-227.

GURLIT 2006
E. Gurlit, 'Die Verfassungsrechtsprechung zur Privatheit im gesellschaftlichen und technologischen Wandel', *RDV* (2006), pp. 43-50

GUSY 2004
C. Gusy, 'Lauschangriff und Grundgesetz', *JuS* (2004), pp. 457-262.

HOLZNAGEL AND BONNEKOH 2006
B. Holznagel and M. Bonnekoh, 'Radio Frequency Identification – Innovation vs. Datenschutz?', *MMR* (1) (2006), pp. 17-23.

ISENSEE 2004
J. Isensee, *Handbuch des Staatsrechts für die Bundesrepublik Deutschland* [Compendium of the Constitutional Law of the Federal Republic of Germany] (Heidelberg, Müller 2004).

JARASS 1995
H. Jarass, 'Bausteine einer umfassenden Grundrechtsdogmatik', 120 *AöR* (1995), pp. 345-381.

[97] BVerfG, 08 *CR* 2005, 569.

JARASS AND PIEROTH 2004
H. Jarass and B. Pieroth, *Grundgesetz für die Bundesrepublik Deutschland – Kommentar* [Commentary of the Constitutional Law of the Federal Republic of Germany] (München, Beck 2004).

KLEWITZ-HOMMELSEN 2003
S. Klewitz-Hommelsen, 'Recht auf Anonymität?', *DuD* (2003), p. 159.

KÖSTER AND JÜRGENS 2006
O. Köster and U. Jürgens, 'Die Haftung von Suchmaschinen für Suchergebnisse', *K&R* (2006), pp. 108-112.

LEUTHEUSSER-SCHNARRENBERGER 2005
S. Leutheusser-Schnarrenberger, 'Der Gesetzentwurf der Bundesregierung zum "großen Lauschangriff"', *ZRP* (1) (2005), pp. 1-3.

LOBER AND WEBER 2003
A. Lober and O. Weber, 'Entgeltliche und freie Nutzung von Persönlichkeitsrechten zu kommerziellen Zwecken im deutschen und englischen Recht', *ZUM* (2003), pp. 658-675.

OGOREK 2004
M. Ogorek, 'Anmerkung VGH Mannheim, Urteil vom 21.7.2003 – 1 S 337/02', *JA* (2004), pp. 608-610.

ROSSNAGEL, ET AL. 1990
A. Rossnagel, et al., *Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik* [Digitalisation of the Basic Rights? On the Constitutionality of Information and Communication Technology] (Opladen, Westdeutscher Verlag 1990).

ROTH-STIELOW 2002
K. Roth-Stielow, 'Stufungen des vorgeburtlichen Lebensschutzes', *ZRP* (2002), p. 530.

SCHAAR 2006
P. Schaar, 'Datenschutz im Spannungsfeld zwischen Privatsphärenschutz, Sicherheit und Informationsfreiheit', *RDV* (2006), pp. 1-6.

SCHMIDT-BLEIBTREU, ET AL. 2004
B. Schmidt-Bleibtreu, et al., *Kommentar zum Grundgesetz* [Commentary of the Basic Law of the Federal Republic of Germany], 10th edn. (Neuwied, Luchterhand 2004).

SPRANGER 2003
T.M. Spranger, 'Biomedizin und vorgeburtlicher Lebensschutz', *SuP* (2003), pp. 71-78.

STENZEL 2006
I. Stenzel, 'Über die Haftung des Metasuchmaschinenbetreibers für die Wiedergabe rechtswidriger Inhalte', *ZUM* (2006), pp. 405-407.

STÜRNER 2005
R. Stürner, 'Caroline-Urteil des BGH: Rückkehr zum richtigen Maß', *AfP* (2005), pp. 213-221.

VON MANGOLDT, ET AL. 2005
H. von Mangoldt, et al., *Kommentar zum Grundgesetz – Band 1* [Commentary of the Basic Law – Vol. 1] (München, Vahlen 2005).

VON MÜNCH AND KUNIG 2000
I. von Münch and P. Kunig, *Grundgesetz-Kommentar, Band 1* [Commentary of the Basic Law, Vol. 1] (München, Beck 2000).

VON STECHOW AND VON FOERSTER 2004
C. von Stechow and M. von Foerster, 'Vereinbarkeit der Videoüberwachung öffentlicher Räume mit dem Recht auf allgemeine Persönlichkeit', *MMR* (2004), p. 202.
WELP 2006
K. Welp, 'Virtuelle Demo. Aufruf zu Online-Sit-Ins ist keine Nötigung', *DFN-Infobrief Recht* (September 2006), available at <http://www.dfn.de/content/fileadmin/3Beratung/Recht/1infobriefearchiv/Infobrief-sept06.pdf>.
WOLF 2005
H. Wolf, 'Anmerkung BAG, Beschluss vom 29.6.2004 – 1 ABR 21/03', *BB* (2005), p.108.
ZAGOURAS AND KÖRBER 2006
G. Zagouras and T. Körber, 'Rechtsfragen des Game-Designs – Die Gestaltung von Computerspielen und –animationen aus medien- und markenrechtlicher Sicht', *WRP* (2006) pp. 680-690.