The End of the "Woodward and Bernstein" Era? The German Constitutional Court and Journalists´ Privacy on Mobile Phones

By Marion Albers and Stefanie Witzke

A. Introduction

In a society in which communication is increasingly mediated by electronic networks the methods of police investigation change. Instead of traditional methods like questioning and plain-view surveillance, the police increasingly prefer the surveillance of communications mediated by networks. The corresponding methods offer possibilities of gaining information which were not available before. Especially if the police use them without preliminary knowledge or a base suspicion at an early stage of the investigation, these methods are characterized by their scope: they result in the collection of a lot of irrelevant information and they affect many uninvolved and innocent persons. But at the same time they may furnish exactly the evidence the police are looking for: the phone number and whereabouts of the suspect; the conversation that verifies participation in an offense. It can be no surprise that these methods have become the central methods of investigation.1

The problem such methods create with respect to the protection of privacy and unobserved communication becomes abundantly clear if journalists are the subject of such surveillance techniques. Modern investigative journalism depends on the use of modern communication instruments like mobile phones. At the same time, it depends on the protection of the secrecy and confidentiality with regard to the contents of communications as well as to the informants. The *Bundesverfassungsgericht* (BVerfG – Federal Constitutional Court) has always emphazised this legitimate interest.2

[1] For numbers and the increase in the use of electronic surveillance in Germany see www.datenschutz.hessen.de/f09set.htm; according to the paper "Transparenz bei der Telefonüberwachung" the number of surveillance measures has increased annually for 25 percent. See also the 19. Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz, www.bfd.bund.de/information/berichte.html. For the increase of wiretaps in the US see the Center for Democracy & Technology www.cdt.org/digi_tele/wiretap-overview.html.

[2] BVerfGE 20, 162 (176); 77, 65 (64 f.); 100, 313 (365).

https://doi.org/10.1017/S207183220001631X Published online by Cambridge University Press

What protection does the *Grundgesetz* (GG – Basic Law) provide for the mobile phone communication of journalists against surveillance by prosecution authorities? On 12 March 2003 the Federal Constitutional Court ruled in two cases dealing with this subject.

B. The Facts

I. Schneider Case

The *Schneider-Case* is linked to an exceptional bank scandal. In the 1980s Dr. Jürgen Schneider managed to obtain credits for a number of inadequately secured projects. The banks were bluffed by his clever behavior as a serious and important businessman. It also appears that the lenders were seduced into taking the risk by the promise of big profits. The scam ran for several years before collapsing and casting Schneider under the suspicion of credit fraud worth a total of several million Euro, fraudulent invocation of bankruptcy and tax evasion. He was therefore wanted by the police worldwide.3

The complainants in the case before the Federal Constitutional Court, the German public TV channel ZDF, and two journalists working for this TV channel, were investigating the Schneider story for the TV program "Frontal." The journalists were trying to develop background information about the Schneider case and they succeeded in getting, allegedly through an informant, an audio cassette with statements of Schneider telling about his business and discussing how easy it was for him to get the loans. On the audio cassette Schneider even presents the thesis that the banks bear joint responsibility for the events.

One of the journalists gave the audio cassette to the *Bundeskriminalamt* (Federal Bureau of Criminal Investigation), which ascertained the authenticity of the recording. Thereupon, at the request of the *Staatsanwaltschaft* (Public Prosecutor), the *Amtsgericht* (Local Court) of *Frankfurt* ordered the disclosure of the connections of the mobile phone which belonged to the TV channel ZDF and was expected to be used by the journalists to get or stay in contact with Schneider. The order was addressed to the mobile phone network provider and was based on section 12 of the Fernmeldeanlagengesetz (FAG -- Law Concerning Telecommunication) and, additionally, on section 100 a and b of the Strafprozessordnung (StPO -- Code of Crimi-

[3] "Baulöwe Schneider in Miami verhaftet", Die Welt, 20.05.1995, also published in www.welt.de/daten/1995/05/20/0520wi110298.htx.

https://doi.org/10.1017/S207183220001631X Published online by Cambridge University Press

nal Procedure). Section 12 FAG permits the competent judge to order information about telecommunications, especially about connection data, in criminal prosecution investigations if facts exist that justify the conclusion that relevant communications originate from the target of such a request. Sections 100 a and b StPO permit the court to order the surveillance of telecommunications, including their contents.

II. Klein Case

The *Klein-Case* is based on journalistic reports about Hans-Joachim Klein who was suspected of being a member of the terrorist movement *Revolutionäre Zellen* (Revolutionary Cells), a movement similar to the *Rote Armee Fraktion* (RAF – Red Army Fraction). Klein was suspected of a triple murder in connection with an assault on the OPEC-Conference in 1975.4 Since then he has been living as a fugitive, lastly in France. Since the end of the 1970s he gave a series of interviews in which he discussed his membership in the RZ and his life after leaving the organization; he condemned terrorism; and he called on persons still involved in such activities to withdraw from terrorist movements. In the meantime the subject of left-wing terrorism has been the subject of permanent public discussion and analysis in Germany.

The complainant before the Federal Constitutional Court involves a journalist working for the weekly news magazine *STERN*, who has published several reports about Hans-Joachim Klein and an interview with him. In 1998 the Public Prosecutor received information suggesting that the journalist was in contact with Klein again. At the request of the Public Prosecutor, the Local Court of *Frankfurt* ordered the disclosure of the connections of the journalist's mobile phone. The order, addressed to the mobile network provider, covered the connection data of the phone calls the journalist made as well as all connection data of all incoming calls. The data gained led to the residence of Klein in France and he was arrested.

III. Procedural History

The appeals against the decisions of the local courts, concerning the access to the journalists' telecommunications connections information, were without success. The courts examining the decisions argued that the right to refuse to produce evidence is limited to certain exceptions, none of which applied to these particular

[4] For further background information of the assault on the OPEC-Conference see "Anschlag auf OPEC-Tagung" in www.rhein-zeitung.de/on/00/10/17/topnews/kleinhin.html.

cases. In particular, the courts found that there was no special privilege for journalists.5

In their constitutional complaints, the complainants alleged an infringement of the secrecy of telecommunications provided by Art. 10.1 of the Basic Law6 and of the freedom of the press and media enshrined in Art. 5.1 of the Basic Law.7

C. The Decisions of the Constitutional Court

The First Senate of the Federal Constitutional Court rejected the constitutional complaints. The Court reaffirmed that the secrecy of telecommunications protects all complainants as well as the freedom of the press and the media. However, the Court concluded that the impairments involved in these cases were justified and that therefore fundamental rights had not been infringed.

I. The Protection Provided by the Secrecy of Telecommunications

The protection of the secrecy of telecommunications covers the protection of the contents of communication as well as its conditions.8 Communication participants adapt themselves and the contents of their communication to each other. The communication would be avoided, reduced or at least changed if the participants knew or feared that state authorities might have tapped their phones and might exploit the acquired knowledge for the states´ purposes. Phone communication are especially exposed to surveillances because - in view of the distance between the communication participants - they rely on communication technologies and operators or providers. In historical and in current perspective the protection of the secrecy of telecommunications mainly refers to security authorities.9 The fundamental right protects against both the taking notice of the occurrance of the communication as

[5] LG Frankfurt, NJW 1996, 1008 et. seq.

[6] "The privacy of correspondence, posts and telecommunications shall be inviolable."

[7] "Every person shall have the right freely to express and disseminate his opinions in speech, writing, and pictures and to inform himself without hinderance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship."

[8] BVerfGE 67, 157 (172); 85, 386 (396); 100, 313 (358 et. seq.); BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Para. 47, http://www.bverfg.de.

[9] BVerfGE 85, 386 (396).

well as the storage and exploitation of the acquired data for purposes defined by the state. The authorities can, especially in connection with additional knowledge, develop useful information even from data which seem to be trivial or harmless. Therefore, the protection includes not only the contents of a protected communication but also the conditions, namely *if*, *when*, *how*, *how often* and *between which persons* a conversation takes place.10

An impairment of this right exists when the state takes notice of the protected communication, stores or uses the data or knowlege extracted from the data. In the cases before the Court, the private mobile network provider had to provide for interception and informed the state authorites about the retained and seperately collected data of the mobile phone connections the complainants had. As the provider was fulfilling an order of a court, the Court explained, the state could be held accountable for the data transmission. In any event, the point is not the data transmission by the provider but the fact that the state authorities subsequently took notice and made use of the transmissions and data or information associated therewith.11

However, this impairment of the secrecy of telecommunications, the Constitutional Court held, is justified. The justification can be drawn from Art. 10.2 of the Basic Law, which allows the limitation of the fundamental right pursuant to acts based on the law.12 But this reservation of restrictions does not allow any and all limitations on the right to telecommunications privacy. Both the legal basis and the restricting act upon which it is based must meet further constitutional requirements provided by the delimited fundamental right and by other relevant constitutional guarantees.

The legal basis has to be in accordance with the constitution. In the present cases, the orders of the local courts were based upon section 12 FAG and, additionally, on sections 100 a, b StPO. Section 12 FAG has been replaced by the new legal standards of sections 100 g, h StPO, but not until the beginning of the year 2002.13

---

[10] BVerfGE 67, 157 (172); 85, 386 (396); 100, 313 (358).

[11] Therefore the protection doesn´t depend on the obligation of the mobile network provider to follow the order. An impairment of the state would exist as well if the provider gave the information voluntary.

[12] "Restrictions may be ordered only pursuant to law."

[13] For any differences between the former and the new law see BT-Drs. 14/7679; *Johann Bizer,* Verpflichtung zur Herausgabe von TK-Verbindungsdaten an den Staatsanwalt, DuD 26 (2002), 237.

And, although conformity with the constitution is an ordinary and obligatory requirement, the Constitutional Court did not examine section 12 FAG nor sections 100 a, b StPO. It conceded that there are doubts about the constitutionality of section 12 FAG. It simply stated, however, that there is no need for a closer look because the complainants had argued not against the legal basis as such, but only against the court orders themselves.14 This constriction of the constitutional review is glaring and cannot be explained by doctrinal considerations. It appears that the Court simply did not want to deal with section 12 FAG or to ascertain its unconstitutionality. Instead, it prefered to annotate the new standards in sections 100 g and 100 h StPO. However, the missing review is problematic as, generally, with the ordinary doctrinal criteria in mind, an unconstitutional legal basis causes the unconstitutionality of decisions under review.

The Court only examined the decisions of the lower courts within the focus of a proportionality test. The principle of proportionality involves the evaluation of four requirements.15

Firstly, the acts under scrutiny have to follow a *legitimate objective*. In the *Schneider-Case* as well as in the *Klein-Case* this was the need for an effective criminal prosecution and a complete clarification of facts, particularly if the offenses under investigation are grave.16

The second requirement is the *suitability* of the chosen means to attain the objective. The Court stated that the order for information about the connection data was suitable to detect the whereabouts of a person likely to be in touch with the user of a mobile phone. In the cases before the Court the suspects were assumed to be in contact with the complainants.17

The third requirement is the *necessity* of the disputed means. The state should not have an alternative at its disposal which would impose less significant hardship with respect to the individual's freedom. The Court pointed out that section 100 a StPO, contrary to section 12 FAG, establishes a principle of subsidiarity at an ab-

---

[14] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Para. 55, http://www.bverfg.de.

[15] See BVerfGE 45, 187 (260 et. seq.); 48, 118 (123 et. seq.); 59, 95 (97).

[16] The Court has emphasized the legitimation of this objective several times, BVerfGE 77, 65 (76); 80, 367 (375); 100, 313 (388 et. seq.).

[17] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 58 et. seq., http://www.bverfg.de.

stract level: phone tapping that permits taking notice of the contents of the protected communication is only allowed if the prosecution authorities have no reasonable chance to detect the whereabouts of a suspect by other means. So the legislature has estimated the disadvantages of an order for information about connection data to be less. The Court considered that this is not objectionable as a general assessment. It concluded that the affirmation of the necessity depends on a weighing of interests in the individual case. In the cases before the Court no less restrictive means were apparent. The Court emphasized that account must be taken of the fact that alternative methods of investigation, *i.e.* a permanent, plain-view observation of the complainants, would have also affected their privacy18

The fourth and last requirement is the *adequacy* of the methods used to obtain information while imposing upon a person's privacy. The disadvantages for the protected freedom must not be dispropriate in comparison with the advantages which can be achieved for the benefit of the common good, namely the criminal prosecution.

On the one hand, the Court admitted that the impairment of the right of secrecy of telecommunications was grave. The intensity of such impairments has increased due to technical innovations. The digitalization of telecommunication permits the computer-controlled production of data records and their automatic storing for the maintenance of the connection and also for accounting purposes. In quantitative respects the digitalization produces a significant amount of data, all the more in light of the integration of networks and telecommunications services. In qualitative respects the connection data make it possible to draw relevant conclusions concerning the communication and movement of the participants to a communication. The entirety of data stored in connection with the phone number can reveal the social environment of the person owning or using the phone as well as the intensity of his of her contacts. The data even may give hints to the contents of the communication. This form of information can be manifest as additional knowledge is available or, like business data, achievable by public registers. The result of surveillance or taking notice of communications by the prosecution autorities, the Court held, could be that the trust in the protection of communication is diluted.19

Specifying the intensity of the impairment, it also has to be considered that the transmission of the connection data by the mobile phone network provider and the

[18] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 61 et. seq., http://www.bverfg.de.

[19] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Para. 71, http://www.bverfg.de; BVerfGE 100, 313 (381).

prosecution's subsequent taking notice and exploitation of the data affects all persons who where connected with the monitored phone. Every order of information is characterized by its spread. In its scope it includes many people who have nothing to do with the assumed offense or with the suspect. Nevertheless, the data transmission and the exploitation by the prosecution exposes them all to the risk that they will become the object of an investigation. This hazard adds to the general risk of being improperly suspected of wrongdoing.20

The intensity of the impairment is underlined by the fact that the data transmission and the exploitation is typically executed secretely, abusing the confidentiality of those concerned. Thus, those affected can only defend themselves against the surveillance by judicial means after the event and if they are informed or find out about it in another way.21

On the other hand, the Court specified the weight of the interest of criminal prosecution by three criteria: It depends on the severity and impact of the assumed offense, which is being investigated. Firstly, the impairment of the secrecy of telecommunications demands a severe offense. The new standards in section 100 g StPO limit the legitimacy of the data collection upon special premises and by pointing to the enumerated offenses in section 100 a StPO. This legal strategy is commonly used in criminal procedural law to limit the use of a method of investigation. At least these standards, the Court held, meet the requirements provided by the principle of proportionality. Secondly, a concrete and, in reference to both the basis of facts and the probability, sufficient suspicion that the suspect has committed the offense is necessary. Finally, a sufficient basis of facts must exist demonstrating that the person affected by an order to obtain information about telecommunications connection data is in touch with the suspect. Pure speculation is not satisfactory.22

Reviewing the decisions before it, the Constitutional Court found in both cases that the offenses investigated were severe. Klein was suspected of a triple murder. In the *Schneider-Case*, the extent of the damage, the number of financially harmed persons and the conditions of the offenses gave evidence of their seriousness, though the legislature did not enumerate them in the catalogue of section 100 a StPO.

---

[20] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 72 et. seq., http://www.bverfg.de.

[21] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 66 et. seq., http://www.bverfg.de.

[22] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 75 et. seq., http://www.bverfg.de.

Therefore the Court stated that the constitutional demands were met in this case as well. In both cases arrest warrants had already been issued. The court ordering the information about the telecommunications connection data could also assume that the complainants had contact with the suspects.23

In the *Klein-Case*, the Court also found the data retrieval concerning the incoming calls to be justified and proportional. The Court, as before, did not review the legal basis, but concentrated on its application.24

The connection data of the incoming calls are not automatically stored for accounting purposes together with the phone number of the called person.25 If the mobile network provider is ordered to give information about the phone numbers of incoming calls the data records of all customers and all stored connection data have to be matched with the phone number of the monitored person. The provider, German Telekom, explained to the Constitutional Court that in 2002 every one of the 216 million connections which have been made every day were party to such a data match on an average of two times.

As this method affects an exceptionally large number of people, the adequate requirement imposes a high threshold for its use. The Court concluded that all those who were ascertained to have had a connection with the monitored phone number and whose data records therefore had been transmitted to the prosecution authorities were impaired in their fundamental right provided by Art. 10.1 of the Basic Law. The data records had subsequently been the starting point of further investigations. Beyond this positive information, the data match included negative information of the kind that all the other checked numbers *had not been* connected with the monitored one (that is, the state had gained knowledge about who they were *not* calling). In this respect, several million persons were affected. As the surveillance of these persons stays anonymous, traceless and without any further interest for the prosecution authorities, the Constitutional Court denied that an impairment of the individual right had resulted on these grounds. However, it emphazised the objective guarantees provided by the fundamental right of the secrecy of telecommunications.26

---

[23] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 80 et. seq., http://www.bverfg.de.

[24] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Para. 92, http://www.bverfg.de.

[25] The reason is that regularly only the calling person has to pay the call.

[26] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Para. 98, http://www.bverfg.de.

Reviewing the challenged decision in the *Klein-Case*, the Court argued that the gravity of the assumed offenses, the concrete suspicion against Klein, the fact that the complainant was highly-likely to be in contact with Klein and the fact that the prosecution authorities had long been thwarted in their attempts to locate Klein, justified the impairment.27

According to the Constitutional Court the reservation of a judicial decision, which is established in section 12 FAG and section 100 b StPO, was not violated.28 The reservation of a judicial decision aims at a preventative supervision of the aspired surveillance by an independent and neutral judicial authority.29 The Constitutional Court did not overlook the fact that, in the *Schneider-Case* as well as in the *Klein-Case*, the justifications for the surveillance provided by the local courts had not fulfilled the constitutional requirements. The courts had only pointed to the existing warrants and to the aim of detecting the whereabouts of the suspects; subsequently they merely repeated the words of section 12 FAG. The Constitutional Court tried to paper over this obvious fault with the argument that, at second instance, the *Landgerichte* (Regional Courts) had given sufficient reasons in reviewing the lower court's decisions.

However, the regional courts regularly only review the orders of the local courts *after* the surveillance has already been carried out. The task and the functioning of the reservation of a judicial decision is to ensure that constitutional requirements are met in the preventative context, prior to the commencement of the surveillance. A higher court cannot correct inadequate reasons for the initial order. The argumentation of the Constitutional Court leads to the result that the reservation of a judicial decision will be undermined.

II. The Protection Provided by the Freedom of Press and Media

The constitutional review addressed in the previous section only referred to the secrecy of telecommunications secured by Art. 10.1 of the Basic Law. The Court dealt with the characteristic that journalists were involved only in its review of Art. 5 of the Basic Law.

---

[27] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Para. 99, http://www.bverfg.de.

[28] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 86 et. seq., http://www.bverfg.de.

[29] BVerfGE 103, 142 (151 et. seq.).

Art. 5.1 of the Basic Law ensures the freedom of press and media. The Constitutional Court has always emphazised the importance of this fundamental right for democracy.30 The scope of protection covers the protection of the institution of the press and media. It reaches from the gaining of information to the spreading of news and opinions. It includes the secrecy of all sources of information and the confidentiality between press or media and their informants. The interest of secrecy of documents that result from journalists' investigations and the contact to the persons being subjects of the coverage are protected as well. Beyond that, Art. 5.1 of the Basic Law embraces the right of secrecy of the editorial staff. This right has an additional importance besides the confidentiality between the media and their informants.31

The challenged orders granting the prosecution the right to acquire information about the connection data of these journalists' mobile phones, the Court held, impaired the freedom of press and media. This impairment can be approved, although the orders of information did not aim at disclosing the identity of an informant but to the whereabouts of a known suspect who was also serving as an informant for the press. The free flow of information between journalists and their informants is already endangered if an informant has to worry about disadvantages due to his communication with the journalists. The Court also emphazised that the challenged orders of information and the data transmission might result in the disclosure of the identity of informants who were anonymous. Besides, the fact that the state had taken notice of the contacts, which took place in the context of journalistic investigations, constituted an impairment of the right of secrecy of the editorial staff.32

However, the Constitutional Court concluded that the impairment of Art. 5.1 of the Basic Law was justified.

The reservation of restrictions entitles the legislature to limit the scope of protection of the fundamental right. However, the restricting Laws as well as the executing acts have to meet the constitutional requirements.

---

[30] BVerfGE 7, 198 (208); 101, 361 (389).

[31] BVerfGE 20, 162 (176, 187 et. seq.); 50, 234 (240); 66, 116 (133 et. seq.); 77, 65 (74 et. seq.); 100, 313 (365); BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 102 et. seq., http://www.bverfg.de.

[32] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 105 et. seq., http://www.bverfg.de.

At first the Court pointed to the special rules the legislature has created to protect journalists in criminal proceedings. Journalists have the right to refuse to produce evidence as long as the identity of an informant or the contents of his or her information is concerned33 With regard to written documents, a corresponding prohibition of confiscation is laid down, if the documents are in the custody of the journalist.34 The Court concluded that the legislature attributed to the aspect of possession of the documents a central role in specifying the protection. In the scope of its decision-making authority the legislature has, according to the Court, gathered the typical conflicts and undertaken a general weighing of interests between the freedom of the press and media on the one hand and the needs of criminal prosecution on the other hand.35

The possessive element is missing if the data concerning the communication or informants are located at a third party, namely the mobile network provider. So the laws do not provide any special protection in these cases. Leaving the decision to the legislature, the Constitutional Court accepted that this solution is in conformity with the freedom of the press and media.36

Looking back on the Court's extensive illuminations concerning the technical innovation and the significant risks they pose, this argumentation is surprising. Though the Court is right in paying attention to the decision-making authority of the legislature, it should not neglect the fact that the legislature has to observe the protection of the restricted fundamental right. The constitutional review should at least include an examination of whether the criteria the legislature has chosen to solve the conflict of interests are convincing and adequate. Possession, as a criterion, is antiquated in view of the technical development.

Outside of the legal exceptions the protection of journalists takes place only in the weighing of interests in the context of the interpretation and application of the legal

[33] Section 53 Abs. 1 Satz 1 Nr. 5 StPO.

[34] Section 97 Abs. 5 StPO.

[35] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 117 et. seq., http://www.bverfg.de.

[36] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 119 et. seq., http://www.bverfg.de.

basis in the individual cases. Especially with respect to the gravity of the offenses the Court did not object to the challenged decisions.37

It is noticeable that the Court did not elaborate on the freedom of the press and media in this context, especially in light of the fact that in both cases the media's role in the formation of the public opinion was also at stake. In this respect, not only the fact that the informants are suspected to have committed offenses is important. The public is interested in the entire social context, in the background of the events and in the different views as well. The fact that the offenses were grave does not diminish the weight of the interests of the press and media; on the contrary, just on account of the gravity of the offenses the public interest in background information is also exceptional. The Constitutional Court did not succeed in promoting the plurality of perspectives that are needed to describe the various meanings information can take in different contexts. In the context of media reports, which contribute to the formation of the public opinion, the meaning is different from that in which the information is used as part of a criminal prosecution. So the Court failed to specify the weight of the protected interest of the media. Maybe the complainants failed to submit sufficient facts and arguments.

D. Conclusion

The decision of the Constitutional Court covers an important subject, and it has disappointed the press and the journalists. Even if one may keep in mind that the press always knows how to emphasize its interests, some points of the criticism are correct. The decision is not convincing in all respects. First of all, the Constitutional Court did not review the legal basis which served as the justification for the challenged orders. One may accept this for pragmatic reasons as the former legal basis (section 12 FAG) has been replaced by new standards (sections 100g, h StPO). However, the restricted review makes a closer look at some constitutional requirements the legal basis has to meet impossible. The Court did not enter at all into the question of whether the legal basis includes sufficient provisions to protect uninvolved persons, *i.e.* interdictions of data exploitations if the surveillance enables the prosecution authorities to gain information about those persons causally. The Court also neglected the task and functioning of the reservation of a judicial decision in assuming that a higher reviewing court could correct, *ex post facto*, a lower court's inadequate reasons for issuing an order granting the prosecution the right to acquire information and thus impairing the relevant constitutional rights. Reviewing

[37] BVerfG, Decision of 12 March 2003, 1 BvR 330/96, and 348/99, Paras. 121 et. seq., http://www.bverfg.de.

the observance of Art. 5.1 of the Basic Law, the Constitutional Court ignored the fact that the criterion the legislature has chosen for outlining a special protection of journalists – possession of documents – is antiquated in view of technical development in this field. And the Court failed in promoting the plurality of perspectives that are needed to present a convincing weighing of interests.

Nevertheless, the decision of the Court formulates some important restrictions on the surveillance of journalists´ mobile phone communication. The requirements - the severity and impact of the assumed offense, the concrete and sufficient suspicion and the sufficient basis of facts that the concerned person is in touch with the suspect - will prevent the hasty issuance of an order permitting the gathering of information about telecommunications connection data. The Constitutional Court has extensively outlined why such orders of information, the data transmission by a mobile network provider and the corresponding taking of notice and exploitation by the authorities lead to a serious impairment of fundamental rights.