THE RIGHT IN CONFIDENTIALITY AND INTEGRITY OF INFORMATION TECHNOLOGY SYSTEMS ACCORDING TO THE GERMAN FEDERAL CONSTITUTIONAL COURT: "OLD WINE IN NEW BOTTLES?"

By Stavros Togias

Abstract

This paper deals with the technical and legal issues raised by the landmark ruling of the German Federal Constitutional Court of February 27th, 2008, holding that the provisions authorising the secret services of North Rhine-Westphalia to employ the special investigative technique of online computer search violates the general right of personality in its particular manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems.

1. Introduction

A wide range of criminal activity –encompassing among others organized crime, right or left-wing extremists and Islamic terrorist groups– uses *information technology* not only for the accomplishment of its propaganda objectives, but also to ensure a principally *secret* communication, ideal for the preparation and execution of criminal plans. On the other hand, law enforcement agencies are standing on the threshold of a new era, facing the risk of being pushed out of the limelight of crime detection, due to the rapid progress of information technology and the prevailing patterns of *conspiration* and *detection-proofing* of criminal networks [Livos, 2007].

Thus, the traditional and routine investigative measures, such as interception of telecommunications, tend to become pointless as modern offenders either refrain from transmitting crime-related information over the telephone or the Internet, or, in the rare case when they do so, they employ elaborated encryption technologies [Hofmann, 2005].

In contrast, the novel *online search* [online Durchsuchung] seems to promise successful investigation of such serious crimes and, likewise, to counteract the aforementioned demerits of outdated investigative techniques. The online search facilitates the *covert* electronic intrusion into the storage media (e.g. hard drive) of the targeted computer *unbeknownst* to its user. This controversial investigative technique appears particularly beneficial with reference to criminal organisations, since it both enables the *prompt* collection of electronic data –i.e. at the preparatory stages of the commission of a felony and before the encryption of the crime-related information [Federrath, 2009]– and does not attract the rest members' of the organisation notice, as it would be the case, if a conventional (physical) search and seizure was performed [Kudlich, 2007].

The *Council of the European Union*, shortly after the delivery of the judgement of the German Federal Constitutional Court [Bundesverfassungsgericht] in the "online search" case, invited the Member States and the Commission to introduce measures based on case studies, particularly taking into account technological developments, so as to prepare tools for operational use, such as "facilitating *remote searches* if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country" [see Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting, Brussels, 27-28 November 2008] [Abel 2009].

2. Factual and technical background

Such secret measures were in the recent past performed in isolated cases –fewer than ten per year, according to the Government of the *Land*– by federal authorities without a specific statutory empowerment and, thus, were temporarily ceased, when the Federal Court of Justice (Bundesgerichtshof) ruled that the Code of Criminal Procedure (Strafprozessordnung - StPO) did not currently provide a sufficient legal basis for their execution (see Decisions of the Federal Court of Justice in Criminal Cases [Entscheidungen des Bundesgerichtshofs in Strafsachen - BGHSt] 51, 211) [Abel und Schafer, 2009].

The political debate in Germany –starring the most outspoken proponent of the measure, Federal Minister of Interior *Schäuble* and his sceptical opponent, Federal Minister of Justice *Zypries*– was conducted in a remarkably lively and sometimes witty manner (see the frontispiece of the former's interview in newspaper *Handelsblatt* of 05.04.2007: "Terrorists do not communicate by carrier pigeons!" [Holzner, 2009]).

Online search is technically feasible via the installation and subsequent activation –usually by sending to the computer concerned an e-mail allegedly originating from a state agency beyond suspicion– of a *Trojan horse* (e.g. the so-called Root-kits) or a *back-door programme*. If, for instance, the person concerned uses a program for receiving real-time stock market information, then the Trojan horse is embedded therein and, hence, the law enforcement agency is facilitated to transfer and review of the data existing in the storage medium of the computer, while the user's account is connected to the Internet (online) [Abel and Schafer, 2009]. As the Court has argued, "insofar as such [ongoing Internet communication] is encrypted as it takes place –this is in particular frequently the case with speech telephony– it can only be effectively monitored at the terminal" [par. 11].

A Trojan horse –a malware that appears to perform a desirable function for the user (e.g. tool or game) but instead facilitates unauthorized access to the user's computer system– can thoroughly monitor and *ab intra* manipulate the communication of the host computer with peripherals, such as monitor, keyboard, or even smart-card readers. Such a malware is suited to erase its digital traces immediately after the successful performance of its attack, for example by self-deleting [Federrath, 2009].

3. Outline

Twenty five years after its landmark judgement in the *National Census Case* (Volkszählungsurteil) and the establishment of the right to "informational self-determination" [Mitrou, 2009], the Court gave birth to a *new* fundamental right in the field of information technology on the occasion of testing the constitutionality of the relevant provisions of the North-Rhine Westphalia Constitution Protection Act [Gesetz über den Verfassungsschutz in Nordrhein-Westfalen - VSG NRW] explicitly authorising the competent intelligence authority to engage in secret infiltration of information technology systems.

The Court concluded that the impugned provisions violate the general right of personality in its particular manifestation as a (rather long-winded) *fundamental right to the guarantee of the confidentiality and integrity of information technology systems* [Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme]. According to its ruling, the aforementioned manifestation protects individuals against intrusion in information technology systems, insofar as the protection is not at all or not adequately guaranteed by other fundamental rights, such as in particular the guarantee of the secrecy of telecommunications or the guarantee of the inviolability of the home, as well as by the right to informational self-determination.

Covert measures in a state based on the rule of law should always be the exception and, likewise, a special justification is required thereof, since, due to the lack of knowledge of the individual concerned of the ongoing procedure, he or she cannot influence by his conduct the course of the investigation.

In respect to its considerable burden of intrusiveness, the secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read, is constitutionally only permissible, if *factual indications exist of a concrete danger to a predominantly important legitimate interest*. Predominantly important are the life, limb and freedom of the individual or such interests of the public, a threat to which affects either the basis or continued existence of the state or the basis of human existence (e.g. the functionality of major parts of existence-ensuring public supply facilities). Further, the preventive measure can be justified even if it cannot be ascertained with sufficient probability that the danger will arise in the near future, insofar as *certain facts indicate a danger posed by specific individuals to the aforementioned predominantly important legitimate interest on a case-by-case basis*. The aforementioned measure must in principle be placed under the reservation of a judicial order. The statute authorising such an intrusion must contain precautions in order to protect the core area of private life.

In a nutshell, (a) the challenged provisions are not compatible with the *principle of the clarity and determinedness of provisions*, insofar as the factual preconditions of the regulated measure cannot be sufficiently derived from the statute, (b) the requirements of the *principle of proportionality in a narrow sense* are not met, since the measures provided for in this norm entail interferences with fundamental rights which are so intensive, that they are disproportionate to the public interest of investigation emerging from the regulated occasion for the encroachment, and (c) the intrusive norms do not provide any suitable *procedural precautions* –i.e. a judicial order or an

equivalent (in terms of independence and neutrality) control mechanism– to protect the inviolable core area of private life.

The new provision of § 20k par. 1 of the "BKA Act" (Act on the Federal Criminal Police Office [Bundeskriminalamt] and the Co-operation between Federal and State Authorities in Criminal Police Matters") authorises the aforementioned state agency to perform "online searches" as a *preventive* counter-terrorism measure. The law-maker has broadly adopted the encroachment's normative preconditions verbatim from the verdict of the First Senate [Bäcker 2009].

4. The "loophole-filling" function of the general right of personality

As the First Senate has ruled, a new anonymous fundamental right is established "in particular in order to counter new types of endangerment which may occur in the course of the scientific and technical progress or changed circumstances" [par. 169]. Previous typical examples of the Court's *creative law-making function*, via the "loophole-filling" function of the general right to personality, are also the right of reply to the media [Recht auf Gegendarstellung im Presserecht], the right to know one's origins [Recht auf Kenntnis der eigenen Abstammung] and the entitlement to rehabilitation [Anspruch auf Resozialisierung] [Manssen, 2009]. As regards the current case, the Court concluded that the existing array of constitutional weapons does not adequately take account of the need for protection arising as a consequence of the unprecedented development of information technology systems.

4.1. The guarantee of the inviolability of the home

The "online search" would not only be constitutionally, but also law-politically *short-lived*, if it was to fall within the concept of the guarantee of inviolability of the home (Article 13 of the Basic Law): the lack of the majority necessary for the amendment of the relevant provision of Basic Law, so that the latter encompasses not only the physical but also the *remote* interference with the sanctity of the home, was the substantial ground underlying the Court's reasoning that "the location of the system is in many cases of no interest for the investigation measure and frequently will not be recognizable even for the authority. This applies in particular to mobile information technology systems such as laptops, Personal Digital Assistants (PDAs) or mobile telephones" [par. 194]. Moreover, the spirit of the guarantee of the inviolability of the private dwellings is the *right to be let alone*; yet, the use of information technology systems serves just the opposite purpose, namely the communication with the outside world [Lepsius, 2008].

4.2. The guarantee of the secrecy of telecommunications

The court has declared that "the fundamental rights protection provided by Article 10 of the Basic Law however does not cover the content and circumstances of the telecommunication stored *subsequent* to completion of the communication in the sphere of a subscriber, insofar as he or she can take their own protective precautions against secret data access. The specific dangers of spatially distanced communication, which are to be averted by secrecy of telecommunication, do not then continue to apply to such data" [par. 185]. The protection of the secrecy of telecommunications

ends at the exact moment the message arrives to the receiver and the transmission process is complete [Lepsius, 2009].

4.3. The right to informational self-determination

Insofar as the citizens reckon on the fact that information technology systems are monitored on a large scale, the collective *confidence* in the information technology – which is of massive social and economic interest– is inevitably tempted. Therefore, the new fundamental right meets the need of protection of the individual's information technology system as a particular safeguarded area of privacy. The starting point of the constitutional protection is the system *itself* –any electronic system which is used for data processing: a definition intentionally open and technically neutral– rather than the stored data therein [Bäcker, 2009]. That is the prevailing reason, why online search does not fall into the scope of protection of the right to informational self-determination.

Moreover, the Court has argued that "the right to informational self-determination does not fully consider elements of personality endangerments which emerge from the fact that the individual relies on the use of information technology systems for his or her personal development and, in such instances, entrusts personal data to the system or inevitably provides such data already by using the system. A third party accessing such a system can obtain data stocks which are potentially extremely large and revealing *without having to rely on further data collection and data processing measures*. In its severity for the personality of the person concerned, such access goes beyond individual data collections against which the right to informational self-determination provides protection" [par. 200]. This ruling reflects the Court's tendency to narrow the scope of the traditional data protection fundamental right, so as to make room for creating a new guarantee –as if the Court no longer trusted the right to informational self-determination to deal with the Internet technicalities and the privacy infringements related thereto [Lepsius, 2008).

5. The case-law of the European Court of Human Rights

Although the concept of an "information technology" right is *expressis verbis* unknown to the European Court of Human Rights, yet the broad interpretation of the notion of the *right to respect for private life*, enshrined in Article 8 of the European Convention on Human Rights, leaves considerable space for the recognition of confidentiality and integrity of information technology systems as important principles underlying such interpretation [Uerpmann-Wittzack, 2009].

In the leading case of *Copland v. the United Kingdom* [no. 62617/00, § 41, ECHR 2007-IV] the Court acknowledged that "the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8".

Further, in the case of the *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (no. 62540/00, § 86, 28 June 2007) the Court criticised "the apparent lack of regulations specifying with an appropriate degree of precision the manner of screening of the intelligence obtained through surveillance, or the

procedures for preserving its *integrity* and *confidentiality* and the procedures for its destruction".

6. Critical assessment

According to some legal commentators the aforementioned right is nothing but a "constitutional fireworks" or an "empty conception" [Bäcker, 2009]. Others contend that the existing constitutional framework of informational self-determination was dogmatically as well as methodologically sufficient enough to preserve privacy under the new pressures from surveillance technology [Manssen, 2009], while some compare the judicial formulation of the aforementioned guarantee to the establishment of the *right to privacy* by the US Supreme Court in 1970's [Lepsius, 2008].

Confidentiality means that information is accessible only to authorised persons, while authorisation refers to a deliberately set up technical access possibility. Likewise, *Solove* [2008] argues: "confidentiality […] consists of sharing the information with a select group of trusted people". On the other side, *integrity* means that information is complete, accurate and up-to-date, or it is clearly noticeable that this is not the case, so the Court, "by the system being accessed such that its performance, functions and storage content can be used by third parties; the crucial technical hurdle for spying, surveillance or manipulation of the system has then been overcome" [par. 204]. However, the Court has not guaranteed the third goal of data protection, i.e. *availability* [Verfügbarkeit] of information: the latter is accessible by the aforementioned authorised persons whenever and wherever there is a need thereof [Hansen and Pfizmann, 2008].

As the Court has observed, new endangerments of personality "emerge from the fact that *complex* information technology systems, such as personal computers, open up a broad spectrum of use possibilities, all of which are associated with the creation, processing and storage of data. This is not only data which computer users create or store deliberately. In the context of the data processing process, information technology systems also create *by themselves* large quantities of further data, which can be evaluated as to the user's conduct and characteristics in the same way as data stored by the user. As a consequence, a large amount of data can be accessed in the working memory and on the storage media of such systems relating to the personal circumstances, social contacts and activities of the user. If this data is *collected* and *evaluated* by third parties, this can be highly illuminating as to the personality of the user, and may even make it possible to form a profile" [par. 178].

Setting aside the fact that collection and evaluation of personal information *are* the privileged field of informational self-determination right –and thus the latter's exclusion from legal instruments adequate to address the issue of secret infiltration of information technology systems seems rather unjustifiable– the First Senate has further noted that "the performance of information technology systems and their significance for the development of personality increase further, if such systems are *networked* with one another. This is increasingly becoming the norm, in particular because of the increased use of the Internet by large groups of the population" [par. 174]. According to a famous quotation of *Scott McNealy* –a legendary character of Silicon Valley– "the Network *is* the Computer" [Böckenförde, 2003]. Most notably, however, as the Court has declared, "the networking of the system opens to third party

a technical access facility, which can be used in order to spy or manipulate data kept on the system" [par. 180]. In other words, protection worthy is per se the *potential* of networked communication, not even the actual creation of individual data traces [Lepsius, 2008].

Thus, the "information technology" fundamental right encompasses either *complex* systems, such as personal computers and smart phones, or simple external storage media (e.g. hard drives or USB-sticks), which, due to their *connection* with another data medium, constitute a sufficiently complex system overall. Accordingly, the new right protects as well virtual hard drives or network-based application programs [Bäcker, 2009].

In this *objective*-orientated context –in contradistinction to the *subjective* structure of the right to informational self-determination– [Lepsius, 2008], the Court has cited as examples of devices that are *not* to be classified as information technology systems, in the sense of its new case-law, non-networked electronic control systems in household appliances or non multifunctional mobile telephones and electronic appointment pads, insofar as such systems due to their technical construction only contain data with a partial connection to a certain area of life of the person concerned [par. 202, 203]. Thereby, the Court comes up against unsolvable *problems of demarcation*: How many functions must a mobile telephone fulfil, so that it ranks among worth-protecting information technology systems? Is redial enough, or address book and folder management are additionally required? What about SMS, Bluetooth, camera or MP3 player? Moreover, the ruling fails to provide a convincing argument for the normative differentiation between an electronic diary and a conventional one: "what is offline illegal can not be online allowed, not even for the State" [Mannsen, 2009].

On the other hand, the Court has lamented that "the constitutional requirements as to the concrete structure of the protection of the core area can differ depending on the nature of the collection of the information and the information collected by it. A statutory empowerment to carry out a surveillance measure which may affect the core area of private life, must ensure as far as possible that no data is collected which relates to the core area. If –as with secret access to an information technology system– it is *practically unavoidable* to obtain information before its reference to the core area can be evaluated, sufficient protection must be ensured in the evaluation phase. In particular, data that is found and collected which refers to the core area must be deleted without delay and its exploitation must be ruled out" [par. 276, 277].

This ruling, addressing the –inherent to information technology and investigative technique– difficulty of an *ex ante* assessment, whether the information secretly accessed is core-area relevant, is of profound importance for the combating of particular aspects of criminality e.g. child-pornography; indeed, even if the person concerned was under concrete suspicion of possessing child-pornography material, under the Court's recent case-law it was a contentious issue, whether the state agents were justified to open a folder titled "Love letters" [Schmidbauer, 2009].

Moreover, the First Senate has demonstrated that the core area of private life is not an obstacle to secret access of the targeted information technology system, "if for instance concrete indications exist that core-area related communication contents are *linked* with contents which fall within the goal of the investigation in order to prevent

surveillance [par. 281]. As an author vividly asserts, “evidently, the Court entertains the idea that clever terrorists seek that their criminal plans evade the state surveillance by intimate whispers with their sexual partners” [Kutscha, 2008].

7. Conclusion and perspective

Information technology has evolved to an autonomous field of performance not only of social or economic activity, but also of new forms of criminal behaviour. Equally, however, information technology constitutes a new, independent field of investigation of network-related delinquency. If the personal computer and the digital information stored therein were until recently the *subject* of investigation, these have already transformed to a prominent *tool* therefore [Böckenförde**,** 2003].

Information Law is the legislator’s answer to the technological revolution that has altered –and keeps altering– the reality of life. More than 20 years ago, an influential academic asserted that “despite the incontestable importance of its technical aspects, *informatization*, like industrialization, is primarily a political and social challenge” [Simitis, 1987]. The legal order, as an instrument expected to provide stability and security to the individuals and society, is hence *structurally* conservative [Uerpmann-Wittzack, 2009]. Yet, the establishment of a new fundamental “information technology” right –to be more precise, a new sub-group of the general personality right [Hornung, 2009]– by the German Federal Constitutional Court is much more than just “relabelling old wine in new bottles”. It rather reflects a comprehensive answer of an *Information Law for the 21st Century* to the relentless questions raised by the rapid technological development and the privacy concerns inherent therewith.

References

German Federal Constitutional Court, Judgment of the First Senate of February 27th, 2008 - 1 BvR 370/07, online at http:/www.bundesverfassungsgericht.de/ entscheidungen/rs20080227_1bvr037007.html/accessed 25.05.2010 (also available in English)

Abel W. (2009), The German “Federal Trojan” – challenges between law and technology, Teutas - Diritto e Tecnologia 2009 (2), 20-32

Abel W., and Schafer B. (2009), The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822, SCRIPTed 6:1 (2009), 106-123

Bäcker M. (2009), Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 1-30

Böckenförde T. (2003), Die Ermittlung im Netz, Tübingen: Mohr Siebeck, 2009

Federrath H. (2009), Technische Aspekte des neuen Grundrechts, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 53-60

Hansen M. and Pfizmann A. (2008), Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, in: F. Roggan (Hrsg.), Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin: BWV Berliner Wissenschafts-Verl., 2008, 131-154

Hofmann M. (2005), Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme? NStZ 2005, 121
Holzner S. (2009), Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, Rechtswissenschaft Bd. 211, Kenzingen: Centaurus-Verl. 2009
Hornung G. (2009), The Online Searching Judgement of February 27th, 2008, in: R. Bendrath/G. Hornung/A. Pfizmann, Surveillance in Germany: Strategies and Counterstrategies, 3-6, online at http://userpage.fu-berlin.de/~bendrath/Bendrath-Hornung-Pfitzmann_Surveillance-in-Germany_2009.pdf/accessed 25.05.2010
Kudlich H. (2007), Zur Zulässigkeit strafprozessualer Online-Durchsuchung, HFR 2007, online at http://www.humboldt-forum-recht.de/deutsch/19-2007/index.html/ accessed 25.05.2010
Kutscha M. (2008), Neue Chancen für die digitale Privatsphäre? in: F. Roggan (Hrsg.), Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin: BWV Berliner Wissenschafts-Verl., 2008, 157-171.
Lepsius O. (2008), Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: F. Roggan (Hrsg.), Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin: BWV Berliner Wissenschafts-Verl., 2008, 21-56
Livos N. (2007), Organised Crime and Special Investigative Techniques, Vol. I: Dogmatics of Organised Crime, Part (a): The criminological-dogmatic phenotype of organised crime, Athens: Law & Economy - P.N. Sakkoulas, 2007
Manssen G. (2009), Das "Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme" – Ein gelungener Beitrag zur Findung unbenannter Freiheitsrechte? in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 61-72
Mitrou L. (2009), The Commodification of the Individual in the Internet Era: Informational Self-determination or "Self-alienation? in: M. Bottis (ed.), Computer Ethics: Philosophical Enquiry. Proceedings of the 8th International Conference, Ionian University, Corfu, June 26-28, Athens: Nomiki Bibliothiki, 2009, 466-484
Schmidbauer W. (2009), Moderne Technik, das Bundesverfassungsgericht und die Polizei – Vorstellungen zur Polizeiarbeit in Computerzeitalter, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 31-51
Simitis S. (1987), Reviewing privacy in an information society, 135 U. Pa. L. Rev. 707 (1987)
Solove D. J. (2009), Understanding privacy, Cambridge: Harvard University Press, 2009
Uerpmann-Wittzack R. (2009), Der Schutz informationstechnischer Systeme nach der Europäischen Menschenrechtskonvention, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 99-109