Regulating Internet Abuses
Invasion of Privacy

Regulating Internet Abuses Invasion of Privacy

Phaedon John Kozyris

KLUWER LAW
INTERNATIONAL

Published by:
Kluwer Law International
P.O. Box 316
2400 AH Alphen aan den Rijn
The Netherlands
E-mail: sales@kluwerlaw.com
Website: http://www.kluwerlaw.com

Sold and Distributed in North, Central and South America by:
Aspen Publishers, Inc.
7201 McKinney Circle,
Frederick, MD 21704,
USA.

Sold and Distributed in all other countries by:
Turpin Distribution Services Ltd.
Stratton Business Park
Pegasus Drive, Biggleswade
Bedfordshire SG18 8TQ
United Kingdom

ISBN 978-90-411-2626-9

Chapter 3

Germany

Spam in the European Union and Germany

*Thomas Hoeren**

1. THE ELECTRONIC ADDRESS AS A 'DATUM OF PERSONAL CHARACTER' IN GERMANY AND UNDER DIRECTIVE 95/46/EC

In Germany, there are two area-specific codes that deal with the processing of personal data in electronic systems. These are the *Mediendienste-Staatsvertrag* (MDStV) and the *Teledienstedatenschutzgesetz* (TDDSG). In addition, the Telecommunications Code (TKG) might be applied. However, there are no court decisions yet and judicial literature is divided on this issue.[1]

None of the aforementioned three codes define what a 'datum of personal character' is. However, there is a definition in the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG), which is to be applied secondarily. According to sec. 3(1) of the BDSG, personal data means any information concerning the

---

* Professor Westfaelische Wilhelms Universitaet.

1. *See* for the context of the following considerations Hoeren, *Neue Juristische Wochenschrift* 2001, 2229 *et seq.*

Phaedon John Kozyris, *Regulating Internet Abuses, Invasion of Privacy*, pp. 57–71.

personal or material circumstances of an identified or identifiable individual (the data subject). When subsuming electronic addresses under this definition, one must differentiate between dynamic and static IP addresses.

1.1. Static Addresses

A Service Provider, who provides Internet access through a static IP address, knows where the computer is located. If the user is a single person or if the provider possesses additional information regarding which individuals use the computer at specific times, this is defined as information concerning the material circumstances of an identifiable individual, i.e. a datum of personal character. If the provider lacks this additional information, the application of the above regime is in dispute. One opinion argues that the wording of the German law does not include primarily technical data. The IP address does not identify the person, but only the computer that is being used. Hence, it does not identify the person unless additional information is known.[2]

The contrary opinion argues that an IP address can at least indirectly identify a person, i.e. the individual becomes identifiable.[3] The main purpose of the data protection clauses, and the reason why 'identifiability' suffices for the definition, would be undermined if the clauses apply only once the allocation list is open. Furthermore, the wording of Art. 2a of the Data Protection Directive ('in particular by reference to an identification number') clearly indicates that the IP address is included in this regime. Finally, the possibility of combining an IP address with a cookie makes it possible for the Service Provider to trace the person's way through the Internet, which facilitates identification. This second opinion is more convincing.

1.2. Dynamic Addresses

If the Access Provider provides the Internet access by giving dynamic electronic addresses, user identification is possible, if the user has to fill in his specific code. If the user is not required to log on with a code, then the Service Provider can only identify him by obtaining the data from the Access Provider. The Access Provider is not allowed to transfer information[4] but might be responsible for this additional information anyway. In this context, the *Amtsgericht Darmstadt* rendered, an

2. Schulz in Roßnagel, *Recht der Multimediadienste*, § 1 TDDSG, 34.
3. Helfrich in Hoeren/Sieber, *Multimedia-Recht* 16.1, 31
4. § 6 TDDSG.

important decision on 1 July 2005.[5] The decision presumes that dynamic electronic addresses are data of a personal character. For this reason, the court prohibited the recording of dynamic electronic addresses by a large company providing telecommunication services (T-Online) for more than 80 days after billing, if the Internet Access contract with the costumer provides for a monthly flat rate. The court has not yet made public its reasons.

1.3. Forwarding Personal Data

As mentioned before, the Provider is not allowed to forward personal data to third persons. An exception is the transmission of dynamic IP addresses (according to the opinion represented here) in the context of felonious or other illegal behaviour.

1.3.1. Copyright Infringement

If copyright rights are infringed upon, the right holder is not entitled to the delivery of the personal data, according to the appellate court in Hamburg.[6] An analogy to § 101 UrhG (Copyright Code) is not possible. The appellate court in Frankfurt (Main) and in Munich came to a similar conclusion.

1.3.2. Law Enforcement

If law enforcement agencies request personal data from the provider, two different legal provisions are implicated. On the one hand, data may be requested according to § 113 TKG which grants such a claim in the case of suspicion of felony, if the right to telecommunications secrecy is not infringed. Under these circumstances there is no need for a prior written warrant by a judge. The regional court (*Landgericht*, LG) in Stuttgart has ruled in this context, that a provider has to produce the name and the address of a costumer.[7] On the other hand, law enforcement agencies can request the disclosure of personal data from the provider on the basis of sec. 100g *et seq*. in conjunction with sec. 100b of the Criminal Procedure Act (StPO – *Strafprozessordnung*). In this case, a warrant by a judge is generally necessary. There is no definitive court decision on the applicability of the two aforementioned claims.

5. Az. 300c 397/04; unpublished.
6. OLG Hamburg: Az. 5 U 156/04; 28 April 2005.
7. Az. 13 Qs. 89/04; printed in NJW (New Juridical Weekly Magazine, No. 09/2005.

2. SUBSCRIPTION CONTRACTS OF INTERNET SERVICE PROVIDERS AND THE QUESTION OF GENERIC CONSENT TO THE USE AND DISCLOSURE TO THIRD PERSONS OF IDENTIFYING DATA

The TDDSG regulates the use and disclosure of personal data in such contracts. Sec. 3 generally prohibits the use and transfer of personal data without consent or permission by this Act or some other regulation.

A general consent is allowed only under certain circumstances:

(a) According to the Data Protection Code it has to be in written form.
(b) Sec. 4 (2) allows for electronic consent under certain conditions: The Service Provider has to make sure that the consent is unambiguous and intended. This consent must be documented, and an opportunity has to be provided for the costumer to withdraw his consent at any time.

With regard to the habitualness of a subscription contract, such generic consent is required as long as it concerns the contractual obligations.

3. SPAM UNDER THE GENERIC CONSENT EXCEPTION

Article 13 (2) of the E-Privacy Directive has been implemented in sec. 7 of the renewed Act against Unfair Competition (UWG – *Gesetz gegen unlauteren Wettbewerb*). According to sec. 7(2), No. 2, of the UWG, the sending of unsolicited commercial messages (in whatever form) is principally seen as an unacceptable nuisance and is therefore prohibited. However, paragraph (3) provides for an exception: direct marketing by e-mail to a costumer is allowed without prior permission of the individual under certain conditions. Thus, an e-mail is not regarded as illegitimate Spam under the following conditions.

Firstly, the advertiser must obtain from his customers their contact details for electronic mail in the context of the sale of a product or a service. Secondly, he is only allowed to use these electronic contact details for the direct marketing of his own similar products or services. Thirdly, the costumers must not have objected to such use (opted out), and fourthly, the customers must be given clearly and distinctly the opportunity to object to such use when their contact details are collected and on the occasion of each further use, without incurring costs other than the transmission costs based on the basic tariff. Under these conditions an unsolicited commercial messages is not regarded as Spam.

However, a problem exists in that sec. 7(3) only mentions customers. Its wording does not include businessmen (tradesmen). Therefore, it is still unclear, whether sec. 7(3) UWG also covers sending e-mails to businessmen e-mail without their prior consent (i.e. the first inquiry about advertisement). An argument for the application of sec. 7(3) regarding businessmen could be that the Data Protection

Directive, apart from protecting natural persons, protects the legitimate interest of enterprises to have functioning networks[8] which might be endangered if sec. 7(3) UWG were not applicable. Others argue that the EU Data Protection Directive, with its regulations against unsolicited commercial messages, seeks to protect individuals from an intrusion into privacy.[9] When Spam reaches tradesmen, there is no such intrusion into privacy, but there is an infringement of sec. 823(1) of the German Civil Code (BGB), which also protects the so-called right of an 'established and protected business enterprise'. Another argument against the application of sec. 7(3) UWG is based on the wording which contains the term 'customer' and not 'market participant'.

In light of the opinion represented here that sec. 7(3) UWG does not protect businessmen, the decision 'E-Mail advertisement' by the German Federal Court of Justice (BGH) has to be considered. According to this decision, which constitutes the first inquiry regarding advertisements, the sending of unsolicited commercial messages to a businessman is allowed 'if an actual interest in the advertisement can be assumed because of concrete circumstances'.[10] At what point a factual interest can be assumed depends on the individual case. Such an assumption may be possible if the sender can presume that receiver's business enterprise might have an interest in certain product information.

4. PROCESSING INFORMATION PUBLICLY AVAILABLE – CONSENT, ACTUAL OR PRESUMED

4.1. Manifest Intent

The two area specific regulations of the *Mediendienste-Staatsvertrag* (MDStV) and the *Teledienstedatenschutzgesetz* (TDDSG) do not deal with this issue. Art. 8 (2) letter e, of the Data Protection Directive has been implemented in sec. 13(2), No. 4, of the Federal Data Protection Code (BDSG). According to this regulation, personal data may be collected without the data subject's participation only if the data has been manifestly made public by the data subject. The requirement that personal data has to be made public 'manifestly' means that the publication is done with the intent of the data subject.[11] An example of publication is mentioning information in a publicly available register.[12]

---

8. Official Journal of the European Union L 201/37, recital 7.
9. Official Journal of the European Union L 201/37, recital 40.
10. BGH, MMR 2004, 386 commented by Hoeren – E-Mail-Werbung.
11. Gola, Peter/Schomerus, Rudolf, BDSG *Bundesdatenschutz* – Commentary, 7th edition, 2002, § 13, Rndr. 18.
12. Gola/Schomerus a. a. O.

4.2. Engaging in Electronic Correspondence as 'Publication'

In this case there is no court decision and the topic has also not been regulated by law.

The intent of the data subject and the person's motivation for joining the electronic communication is the key issue. If the data subject makes an email address available to third persons, then this is a 'publication' in the sense of the regulation, e.g., the e-mail address is being indicated in an 'About Us', 'Contact' or 'Legal Notice' of a homepage, or the person has signed in to lists available on the Internet. Using an e-mail address for individual communication, however, is not publication.

4.3. The Extent of the 'Right to Object'

Generally, collection is only permitted, if it is allowed by regulation or if the data subject has agreed. Despite sec. 13(2) No. 4, BDSG, the general protection clauses remain effective.[13] The right of objection under Art. 14 b of the Data Protection Directive concerns processing personal data for direct marketing. Since the general protection clauses remain in effect, the data subject maintains the right to object in the case of direct marketing using publicly available data. Preserving this right is also emphasized by the renewed Act Against Unfair Competition (UWG – *Gesetz gegen unlauteren Wettbewerb*) and by sec. 7(2) No. 3 UWG. According to this latter section, electronic marketing without the prior consent of the data subject is not permitted. Only under the very narrow conditions set forth in sec. 7(3) UWG, is consent not required. However, this section also prescribes that if the recipient has objected to the sending, sending electronic advertisement is not allowed. Hence, it does not make a difference whether the advertiser has gained the information from a contract or from a publicly available source. Eventually, the right to object is upheld.

5. RELATIONSHIP OF DIRECTIVE 95/46/EC TO DIRECTIVE 97/07/3C ON THE PROTECTION OF CONSUMERS IN RESPECT OF DISTANCE CONTRACTS

These Directives have different focuses and therefore treat the Spam problem from different points of view. Directive 95/46/EC on Data Protection marks the limits of using personal data; the Consumer Directive protects consumers from intrusiveness. The reason for the prohibition of direct-marketing via voicemail and fax

13. Gola/Schomerus § 13, Rndr. 18.

machine under Directive 97/07/EC is the high degree of annoyance and the immense violation of the consumer's privacy. Because of this intended purpose there is no room for any exceptions. In 1997, Spam was already a problem, but not of today's dimensions. As the Directive only wanted to mark the limits of direct-marketing, email was not mentioned. By now, the situation has changed, the Spam problem has increased and the private use of e-mail has become even more popular. For this reason, the new Directive 02/58/EC includes the prohibition of direct-marketing via e-mail.

In order to use fax machines and voice mails for individual communication with a customer one simply needs the customer's consent. If a customer has started a dialogue, he will expect an answer from the entrepreneur. Even without an express compliance via voicemail or fax machine (or e-mail following Directive 02/58/EC), the customer will not enjoy the law's protections any more. A contact that is started by the costumer himself can always be seen as consent.

In Germany, sec. 7 UWG says that direct marketing via phone call needs an express compliance before calling a consumer. For calls to another market participant, a presumptive compliance suffices. Direct marketing via fax, automated telephone machines or e-mail is prohibited without prior consent. Concerning e-mail, there is an exception in sec. 7(3) UWG: advertising via e-mail is permitted, if the seller obtains the e-mail address in the context of a deal, if he uses the address for similar products, if the customer has not disagreed and has been informed about the use of his e-mail address and about his right to recall this use at any time.

6. PROTECTING SENDER OR RECEIVER 'ANONYMITY' ON THE INTERNET

In Germany, laws from different purviews either preserve or prevent 'anonymity' on the Internet. The law against unfair competition does not allow the sending of anonymous Spam mail. According to section 7(2) of the Act against Unfair Competition (UWG), there is an unacceptable nuisance in particular:

(a) Where it is apparent for the advertiser that the recipient does not wish to receive advertisements
(b) Where telephone calls are directed at consumers who have not given their explicit consent to receive such communications (opted in) or where they are directed at other market participants without at least their assumed consent
(c) In cases of automatic calling machines, fax machines or electronic mail being used where the recipients have not given their prior consent; this applies both to consumers and to other market participants, so even if the recipient is not a consumer an assumed agreement will not suffice in this case
(d) Where the identity of the sender on whose behalf the communication is made is disguised or concealed (anonymous communications) or where no

> valid address is given to which the recipient may send a request that such communications cease, without incurring costs other than the transmission costs based on the basic tariff Whoever disguises or conceals his address or indicates no valid address to which the recipient may send his demand to stop such messages, acts in an unfair, i.e. illegal way. Hence, competitors must not anonymise or pseudonymise advertisement messages. The right to anonymity in business is restricted to the consumer. Hence, these rules restrict the right of the senders of e-mail, which must not be anonymous. By the particulars contained in No. 2-4, article 13 of the Electronic Data Protection Directive (02/58/EC) is implemented. Illegal advertisements support a claim for injunction and deletion of the consequences of illegal behaviour[14] or damages[15] against the advertising business enterprises.

Furthermore, Internet Service Providers in Germany are bound by the regulations on data protection of the Teleservices Data Protection Act (TDDSG). Sec. 4 of the TDDSG prescribes: the Service Provider has to enable the user to use teleservice and its billing anonymously or under a pseudonym, as far as this is technically possible and reasonable. Anonymity is also guaranteed by the telecommunications secrecy under sec. 88 of the Telecommunications Act (TKG) which is binding on service providers. According to sec. 88(1) TKG, the fact that someone has participated in a telecommunication process, falls under the secrecy of telecommunications. The connection data of the communication is thus protected. This includes, who has communicated and when, with whom, how long, from where, to where, and in which way. This information must not be transmitted and may be saved only under certain circumstances.

On the other hand, whoever uses his homepage as a media service or a commercial teleservice, is obliged to abide by the duty to give information on the provider according to the TDG and the MDStV. For the private sphere (which is not regulated by the directive 00/31/EG) the right of anonymity is part of the so called general personal right ('*Allgemeines Persönlichkeitsrecht*'), which has been deduced from article 2(1) and article 1(1) of the Constitution (GG) as an undefined freedom right, i.e. a basic right. Everyone has the right to publish anonymously or under a pseudonym in an Internet forum.

7. UNSOLICITED COMMERICAL MESSAGES AND THE AFFIRMATIVE OBLIGATION OF SERVICE PROVIDERS TO CREATE AND MAINTAIN GENERAL 'NO-SPAM' REGISTERS

Recital 31 of Directive 00/31/EC states: Member States which allow the sending of unsolicited commercial communications by electronic mail without prior consent

14. Sec. 8 UWG.
15. Sec. 9 UWG.

of the recipient by service providers established in their territory have to ensure that the service providers consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves. Thus, there is an obligation to create and maintain a general 'no-Spam' register, if the Member States chose the opt-out principle. In Germany there is no such obligation, because the opt-in principle was implemented.

Directive 02/58 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. 37 (L. 201) (E-Privacy Directive)[16]

8. THE 'SPECIFIC' AND 'EXPLICIT' CONSENT REQUIREMENT – SUFFICIENCY OF WILLINGNESS EXPRESSED UPON VISITING A WEBSITE

According to Directive 02/58/EC[17], consent can be given in any adequate way through which the costumer's wish expresses itself in a specific indication given in an informed and free decision; this can also be achieved by marking a field on an Internet website. In Germany, consent to a usually unacceptable e-mail advertisement requires that the e-mail be requested by the recipient. As to the consent of the recipient, the sender principally has the burden of proof. If not explicitly given, consent can only result from the actual circumstances. The potential interest of the recipient for the offered service does not suffice to justify such actual circumstances. The publication of an e-mail address for example does not constitute consent to receive an e-mail advertisement. Visiting a website is also not considered consent. Without explicit consent, the sending of advertisement mail is only allowed under the circumstances of Sec 7(3) UWG.

Sec 7(3) UWG regulates the conditions for sending advertisements by electronic mail without explicit consent. It is an exception clause to paragraph (2), No. 3. Sec 7(3) UWG which implements Art. 13(2) of Directive 2002/58/EC. Article 13 (2) provides that if a person obtains from his customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of similar products or services. However, this exception applies only when the customers clearly and distinctly are given the opportunity to object to such use of electronic contact details, free of charge and in an easy manner. The customer must have the possibility to initially refuse such use and to refuse on the occasion of each message.

16. *Also cf.* prior Directive 97/66, which it replaces.
17. Art. 17.

Sec 7(3) UWG states: 'Deviant to paragraph 2 No. 3 direct marketing by e-mail is not regarded as unfair competition where

(a) the advertiser has obtained from his customers their contact details for electronic mail in the context of the sale of a product or a service,
(b) the advertiser uses these electronic contact details for the direct marketing of his own similar products or services,
(c) the customers have not objected to such use (opted out), and
(d) the customers clearly and distinctly are given the opportunity to object to such use when their contact details are collected and on the occasion of each further use, without incurring costs other than the transmission costs based on the basic tariff.

These four conditions have to be fulfilled, so that the advertiser is ruled by the so called 'soft opt-in' regulation. Conditions (a) and (b) narrow the area of application of this regulation noticeably, because the advertiser has to have contact with the recipient and may only advertise similar products or services.

9. 'NO-SPAM' REGISTERS ALLOWING FOR A GENERIC OPT-OUT

In Germany, there is no obligation to create a 'no-Spam' register, as the opt-in alternative was chosen. Only Member States which chose the opt-out Principle are obliged to maintain a 'no-Spam' register, so-called Robinson Lists (Directive 00/31/EC Art. 31).

10. SOLICITATIONS TO CONSENT AS SPAM

A distinction has to be made as to whether or not there is a business relation between the advertiser and the recipient.

10.1. No Business Relation

There is no court decision yet and there is also no explicit article in the Code. However, the appellate court Karlsruhe[18] and the regional court Karlsruhe[19] had to decide a similar case. The decisions dealt with the question whether the sending of one single e-mail is prohibited. The regional court Karlsruhe found no violation because the interference by only one unsolicited commercial message (Spam) is not serious enough to justify an injunction. The appellate court Karlsruhe ruled similarly and denied an interim injunction. However, both decisions may be not

18. OLG Karlsruhe, MMR 2003, 590.
19. LG Karlsruhe, MMR 2002, 402.

good law anymore because the Federal Court of Justice (BGH), in its decision 'E-Mail Advertisement', has stated explicitly that an action is prohibited if it contains 'the germ to expand further'.[20] If the unsolicited inquiry regarding advertisements were not prohibited, other enterprises, that until now refrained from doing so, might also send such inquiries. As a consequence, the customers/tradesmen would receive many such inquiries. Such a ruling would lead to the expansion considered prohibited by the BGH. Hence, an unsolicited inquiry to send advertisements is a prohibited advertisement.

10.2. Business Relation

Article 13(2) of the E-Privacy Directive has been implemented in sec. 7 of the renewed Act against Unfair Competition (UWG – *Gesetz gegen unlauteren Wettbewerb*). According to sec. 7(2), No. 2, of the UWG, the sending of unsolicited commercial messages (in whatever form) is principally seen as an unacceptable nuisance and is therefore prohibited. However, paragraph (3) provides for an exception: direct marketing by e-mail to a costumer is allowed without prior permission of the individual under certain conditions. An e-mail is not regarded as illegitimate Spam under the following conditions. Firstly, the advertiser must obtain from his customers their contact details for electronic mail in the context of the sale of a product or a service. Secondly, he may only use these electronic contact details for the direct marketing of his own similar products or services. The costumer thirdly must not have objected to such use (opted out), and fourthly, the customers clearly and distinctly must be given the opportunity to object to such use when their contact details are collected and on the occasion of each further use, without incurring costs other than the transmission costs based on the basic tariff. Under these conditions an unsolicited commercial messages is not regarded as Spam.

However, a problem is that sec. 7(3) only mentions customers. Its wording does not include businessmen (tradesmen). Therefore, it is still unclear, whether sec. 7(3) UWG also covers the sending of e-mails to a businessman without his prior consent (i.e. the first inquiry about advertisement). An argument for the application, of sec. 7(3), regarding businessmen could be that the Data Protection Directive, apart from protecting natural persons, also protects the legitimate interest of enterprises to have functioning networks which might be endangered if sec. 7(3) UWG were not applicable. An objection to this argument is that the Data Protection Directive with its regulations against unsolicited commercial messages wants to protect from an intrusion into privacy.[21] When Spam reaches tradesmen, there is no such intrusion into privacy, there is only an infringement of sec. 823(1) of the German Civil Code (BGB), which also protects the so called right of an 'established and protected business enterprise'. Another argument against the

20. BGH, MMR 2004, 346 commented by Hoeren – E-Mail-Werbung.
21. Recital 40.

application of sec. 7(3) UWG is the wording, which contains the term 'customer' and not 'market participant'.

Based upon the opinion represented here that sec. 7(3) UWG does not protect businessmen, the decision 'E-Mail advertisement' by the German Federal Court of Justice (BGH) has to be considered. According to this decision, the sending of unsolicited commercial messages, which also include the first inquiry about advertisement, to a businessman, is allowed, 'if an actual interest in the advertisement can be assumed because of concrete circumstances'.[22] At which point a factual interest can be assumed depends on the individual case. Such an assumption may be possible if the sender can presume that the receiver's business enterprise might have an interest in certain product information.

11. UNSOLICITED COMMERCIAL MESSAGES UPON VISITING A WEBSITE

Advertisement pop-ups and banners on websites do not fall under the regime of Art. 13 of the Directive 2002/58/EC. Art. 13(1) only concerns the use of automatic calling machines, facsimile machines (fax) or electronic mail for the purposes of direct marketing. Direct marketing in e-mail is also not directly comparable to direct marketing by advertisement pop-ups and banners on websites. Usually the user contacts the website voluntarily and is confronted with the advertisement in this context. This is comparable to the purchase of a magazine containing advertisement pages. Just like printed press the gratuitous websites are financed by advertisement. It is the user's decision, whether or not he wants to accept these offers. This situation is different in the case of direct marketing via e-mail. In that case, the owner of the e-mail account generally is confronted with advertisement messages without having acted himself and without his consent. It is consequential to adopt the opt-in principle in the case of email advertisement, because the sending thus occurs with the account owners consent. Visiting a website is based on the user's initiative, and he has the free choice to expose himself to the advertisement by visiting the website or not. As he exposes himself to the advertisement and there is no active advertisement towards him, the question of consent does not arise. An opt-out possibility for website visitors can hardly be enforced as there must be a possibility to identify the user. This regularly is only possible by using cookies and hence only possible with respect to the utilized computer. Apart from the problems concerning data protection when using cookies it is also questionable if such a possibility to opt-out is practically necessary. Through his browser the user has the possibility to block pop-up windows. Standard inter-security-programmes nowadays provide for a blocking function of advertisement banners. Because of the technical difficulty of utilizing opt-out choices and because of the easy and

22. BGH, MMR 2004, 386 commented by Hoeren – E-Mail-Werbung.

cost-efficient possibility to block such advertisements, a rule to prescribe an opt-out option does not appear very reasonable.

12. TECHNICAL AND ECONOMIC FEASIBILITY OF CERTAIN SOLUTIONS

12.1. Require Service Providers to Forward Electronic Mail Only from Listed and Identifiable Sources

It might be, of course, technically feasible to filtre emails before they are forwarded by the provider. A significant economic problem exists because no method of filtring will be safe enough to guarantee that only Spam mail will be sorted out. As soon as 'real' emails are not delivered because of false filtring, the whole reliability of email will be in danger. Providers who use such pre-filtring methods would probably soon lose their customers.

But there is also a legal problem. In Germany, § 206 Abs. 2 Nr. 2 StGB (penal code) prohibits firms that work in telecommunications or mail delivery to eliminate entrusted mailings. The penalty is up to a five year prison sentence or fine. Pre-filtring also called blacklisting is an infringement of this paragraph even if the addressee has allowed for blacklisting. Only if both, addressee and addresser have declared their consent is a justification for this practice possible.

12.2. Require Senders to Pay a 'Spam Stamp' or Answer a Simple Question

12.2.1. Spam Stamp

The idea to install a 'Spam-stamp' is in principle a good approach to reducing Spam. By requesting a minimal amount e.g. EUR 0, 01, the ordinary user of e-mail services is barely burdened. Spam-senders who send up to 5 Mio. email would then have to pay a total amount of 50,000 € (when sending 5 Mio. e-mail). The business model of Spam-senders would be fundamentally undermined. Technically the introduction of a 'Spam stamp' should be feasible; particularly attention should be turned to the elimination of any possibilities of evasion or abuse. However, the problems will lie in the organizational implementation of a 'Spam stamp'. It is a question who will collect it and who will control the proper prepayment. Because of the very low fee for each e-mail, the administrative costs for the collection will be higher than the price for the purchased stamp. This problem cannot be solved by only charging when a certain amount of mail is reached monthly, or based upon a certain data volume. To check the necessary conditions of a prepayment obligation in each case would create additional administrative effort with additional costs.

Thus this concept will hardly be feasible because it lacks a justifiable cost to benefit ratio.

12.2.2. Answering a Question

According to this concept, the sender is authenticated by answering a question. This solution however has the disadvantage that it hinders the automatic sending of e-mail because it requires a logical action by a person. In fact, many Spam e-mails are sent automatically by the accordant software. The automatic sending is in other contexts (e.g. to install an auto-reply function) indispensable. This concept is thus not an appropriate solution for the Spamming problem.

12.2.3. Have Service Providers Require Subscribers to Provide Identifying Data to Enable Tracing

Once again there is no doubt about the technical feasibility of getting all this information from a provider's customer, but again there are economical and legal limits. Customers, especially those who are up to Spam, will change their providers, if such requirements for Internet access were adopted. From the legal point of view it also seems to be impossible to require providers to obtain all of this information. The Directive of Data Protection 95/46 says in Article 6 S. 1 c, that data collection is only permitted for the purpose needed. Following Article 7 b of the Directive such a purpose could be the performance of a contract. However, for the contract between provider and customer one does not need any passwords or electronic signatures. The only way to make this kind of data collection legal is through the creation of a legal obligation. Then Article 7 c would allow the data collection which is needed. In Germany one principle of data protection law is the avoidance of data. Only very essential data should be collected.

The TDDSG (*Teledienstedatenschutzgesetz*), which is applicable for all online-services, differentiates between stock data and use data. While stock data is the kind of personal data that might be collected for the contract,[23] use data includes the user's identification, the duration and amount of each use and the used teleservices. These dates may only be collected as far as they are essential for the use itself and for billing purposes. Therefore, there is no use data collection permitted if customers use DSL-connections which are billed at flat-rates per month. The TKG (*Telekommunikationsgesetz*), which is applicable for pure telecommunication services, contains a similar rule. Here, the differentiation runs between stock data and traffic data. According to § 96 TKG traffic data may only be collected if it is necessary for the connection itself or for billing. If collected data is not necessary for another connection, it has to be deleted immediately.

---

23. § 5 TDDSG.

13. PROTECTION OF WEBSITES FROM SPAM ATTACKS

The anti-Spamming regulation stipulates that there must be an opt-in system for e-mail. Direct-marketing via e-mail is, therefore, only permitted if the receiver has agreed. Websites themselves are not protected by this regulation as they are not receivers of email. Attacks on websites by overwhelming them with inquiries are not covered. The anti-Spamming regulation is just about email. Inquiries may be directed at websites, no matter whether the websites are owner-controlled or not. It is assumed, that websites which offer a form to interpellate have automatically consented to incoming inquiries.

14. ELIMINATION OF OPEN RELAYS AND PROXIES AS A SOLUTION

An open SMTP relay is a mail server which accepts e-mail for any recipient and relays it. Open proxies and routers, which transfer TCP-connections from Port 25 (SMTP) still on TCP-level directly to other mail servers, are subsumed under this term. Because of their openness, these computers are abused by Spammers who transfer advertisement e-mails under a false identity. Reasons for this regularly unintended openness most often are a lack of awareness on the part of the server, a deficient administration, or the usage of outdated software. Spam senders usually find such deficiently secured computers systematically by using special software. They then utilize these computers for their purposes. To achieve this, the Spammer only has to send the advertisement mail with the according recipients by using the security hole to the open SMTP-relay. The relay sends the advertisement mails and in doing so spent system resources and the traffic costs are paid by the server. Free use and the possibility to disguise the e-mail origin make open SMTP relays so attractive for Spam senders. Filling all these security holes would reduce the Spam problem dramatically. However, this is illusory, because making the servers secure is the responsibility of each server. Due to the mass of servers, corrupt administration in various cases cannot be excluded.[24]

24. For the context of this paper *see* Hoeren, *Neue Juristische Wochenschrift* 2001, 2229 ff.