COMPARATIVE ANALYSIS BETWEEN SPANISH AND GERMAN LAW CONCERNING DATA PROTECTION IN INTERNET.[1]

Juan Antonio Mayol Gil
Rafael Medrán Vioque
Manfred Mieskes
Alfonso Ortega Giménez

[1] Socrates Project. “Information Society and Intellectual Property Law”.

I. Introduction.

1. As a result of the rapid development in computer technology large quantities of information relating to individuals ("personal data") are routinely collected and used by public administrations and in every sector of business.

Several Member states of the European Union have since the 1970s passed legislation protecting the fundamental rights of individuals and in particular their right to privacy from abuses resulting from the processing (for example, the collection, the use, the storage, etc.) of personal data. International institutions such as the United Nations, the Organisation for Economic Cooperation and Development (OECD) and the Council of Europe have produced legal texts addressing these issues. A Council of Europe convention (Treaty 108 of 1981) establishes the basic principles regarding the protection of individuals with regard to the processing of personal data which can be found in all data protection laws in Europe.

Data protection laws provide for a series of rights for individuals such as the right to receive certain information whenever data are collected, the right of access to the data, and if necessary, the right to have the data corrected, and the right to object to certain types of data processing. These laws generally demand good data management practices on the part of the entities that process data ("data controllers") and include a series of obligations. These include the obligation to use personal data for specified, explicit and legitimate purposes, the obligation to guarantee the security of the data against accidental or unauthorised access or manipulation and in some cases the obligation to notify a specific independent supervisory body before carrying out all or certain types of data processing operations. These laws normally provide for certain safeguards or special procedures to be applied in case of transfers of data abroad.

Although national data protection laws are to a certain extent similar, a number of differences exist between them. The level of protection guaranteed to the citizens in the Member States is not uniform (two Member states are still in the process of passing data protection laws). This situation creates potential obstacles to the free flow of information and additional burdens for economic operators and citizens, such as the need to register or be authorised to process data by supervisory authorities in several member Sates, the need to comply with different standards and the possibility to be restricted from transferring data in other member states of the EU.

Furthermore the development of a frontier free internal market and the development of the so called "information society" imply that processing of personal data grows irrespective of national boundaries and that the data concerning the citizens of one Member State are increasingly processed in other Member Sates of the EU.

In order to remove the obstacles to the free movement of data while guaranteeing the protection of the right to privacy, Directive 95/46/EC aims at harmonising the national provisions in this field. The right to privacy of citizens will therefore have equivalent protection across the Union. The fifteen member States of the EU are required to put their national legislation in line with the provisions of the Directive by 24th October 1998.

II. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

II.1. Introduction.

2. On October 24th, 1995, the Council and Parliament of the European Union adopted a Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("data protection Directive").

A key objective of the data protection Directive was to allow the free flow of personal data between Member Sates by harmonising the level of adequate protection granted to individuals. The Directive sets forth the applicable law, conditions for data processing, information to be given to the data subject, the latter's right of access, object, confidentiality and security of processing, obligation of notification and content of such notification, as well as the limitations to the transfer of data to third countries imposed within the harmonised scope.

A great value has been placed in the individual's consent, as well as his entitlement to full and fair information on the collection and use of personally identifiable data, the right to access and correct such data, and the right to oppose the user or distribution of such data for marketing purposes.

Beside, the Directive encourages the drawing up of codes of conduct intended to contribute to the proper implementation on the national provisions.

The Directive also requires that any third country to which data are transferred provides "adequate" data protection. Such requirement has been the reason for a delay on its entry into force and the undertaken of negotiations with the US leading to current "safe harbor" proposal.

The Directive 95/46/EC has been complemented by a Directive 97/66/EC of 15 December 1997 on the protection of personal data in the field of telecommunications.

II.2. General rules on the lawfulness of the processing of personal data.

3. The Directive 95/46/EC dedicates its Chapter II, mainly in the articles from 5 to 21, to list the limits by means of which the States will establish the general rules on the lawfulness of the processing of personal data.

In the Section I (article 6) are established the principles relating to data quality. We could see that the data must be processed fairly and lawfully; these data collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible if Member States provide appropriate safeguards; the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; in addition to, the data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; the data will be kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

In the Section II (article 7), it is enumerated the circumstances under which it is possible to realise a data processing. Personal data may be processed only if the data subject has unambiguously given its consent, or it is necessary for the performance of a contract in which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or it is necessary for compliance with a legal obligation to which the controller is subject, or it is necessary to protect the vital interests of the data subject, or it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

The Section III (articles 8 and 9) is dedicated to special categories of processing; those categories are special as a consequence of kind of data that they use. For that reason is forbidden unambiguously the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

The explicit consent given by the data subject to the processing of those data, except where the laws of the Member State provide that the prohibition may not be lifted by the data subject's giving his consent, or it is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or it is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with the organisation in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects, or if the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

The data processing also are exempt when it has a relation with preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and when those data are processed by a health professional subject under national law to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. Moreover the Directive lets an open clause that allows to the Member States add another exceptions. Processing of data relating to offences, criminal convictions or security measures may only be carried out under the control of official authority, however, a complete register of criminal convictions may only be kept under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official and private authorities.

The Section IV (articles 10 and 11) whose title is information to be given to the data subject, makes a list about the information that the data subject should received from the controller or his representative.

The identity of the controller and of his representative, if any, the purposes of the processing for which the data are intended, any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him, and any further information is necessary to guarantee fair processing in respect of the data subject.

On the other hand, when the information is not been obtained of the own data subject, and they are going to be an object of transfer to the third one they will have to report, at the longest in the

moment of the first communication of information, the same information as if the data should obtain of the same data subject.

This information, which must be facilitated to the data subject, was not being applied when the treatment is with statistical purposes or of historical scientific investigation, if it turns out to be impossible or it is required disproportionate efforts the communication to the data subject, for the record or the communication with third, they are prescribed by the law. However, it is recommended that the Members States establish the appropriate guarantees.

The Section V (article 12) treats the right of access to the information on the part of the data subject, who will be guaranteed by the Members States. This right of access consists of the possibility of obtaining of the controller of free form, without restrictions, of periodic form, without arrears or excessive expenses, the treatment or not that of his data is carrying out, the purposes of the treatment, the categories of information that are analysed and to whom they report. All this information will have to be realized so that it will be understandable for the data subject. Likewise, it will have to put in knowledge of the data subject the logic that is used for the treatment of his data, as minimum in those treatments that produce on the data subject juridical effects or affect him of significant way.

The section VI (article 13) limits the right of access of the data subject by means of the following limitations and exceptions:

"a) National security;
b) defence;
c) public security;
d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
g) the protection of the data subject or of the rights and freedoms of others".

Besides, the data will not be able to be used so that they imply measurements or decisions relative to concrete persons. Except when they are going to treat only with the limits of scientific investigation and providing that the period during which they guard these files does not overcome the necessary one for the production of statistics.

The Section VII (articles 14 and 15), recognizes the data subject the right of opposition for legitimate reasons, except in the cases in which there will be reasons of public or it will be necessary for the satisfaction of a legitimate interest of any third one. Also they will be able to be opposed, previous request and without expenses, to the treatment of personal data, when this information is going to be used by the controller for an exploration.

Moreover, the Members states will have to take the necessary measurements in order to the in data subjects know the existence of this right.

The Members States will guard that the persons are not submitted to decisions that produce juridical effects on them or that affect them of significant form, when it is based only on an automated treatment of data that evaluates their personality, their credit, reliability, conduct, etc. This prohibition remains limited by the autonomy of the will or for a law that establishes measurements that guarantee the legitimate interest of the data subject.

The section VIII (articles 16 and 17) tries to guarantee the confidentiality of the information so that they will only be able to treat personal information for indication of the controller or for legal imperative.

The Directive 95/46/EC makes relapse on the controller the application of the necessary measurements of safety to protect the personal data, understanding this protection in a wide sense, that is to say, access, diffusion, modification, etc.

The safety level will have to be in agreement with the technical existing knowledge, the cost and the risks that the data processing presents, it means, to bigger sensibility of the information lesser the cost will influence the safety level that has to be applied.

The controller will have to choose a processor and who will have to gather the sufficient guarantees to guarantee the technical safety and the organization of the treatments that are realized. When the treatments are realized by order, these will have to be regulated by a juridical act that links the processor with the controller, and especially this juridical act will indicate that the processor only actuates following the instructions of the controller and that the safety obligations will must be fulfilled also for the processor, following the State legislation. The measurements relating to the safety will consist in writing or of equivalent form.

The Directive 95/46/EC, in the Section IX of the Chapter II (articles 18, 19, 20 and 21) arranges that the controller or his representative, are bound to notify to the authority of control of the beginning of a treatment or set of treatments, when these are total or partially automated and prosecute a concrete purpose.

The Directive 95/46/EC contemplate the possibility of simplifying or to omit the notification in a few certain cases as the treatment of categories that can not affect the rights and freedoms of the data subjects, having knowledge that the data that they handle, the purpose, the addressees and the period of conservation of the information and/or when the processor of the data takes as an assignment the application of the national regulations adopted by virtue of the present Directive, or take a record of the treatments effected by the controller, hereby to guarantee the rights and freedoms of the data subjects.

Remain exempted of the obligation of notification those treatments that for legal or regulation dispositions take as a purpose to carry out a record of information to the public and open to general consultation whose demonstrates a legitimate interest.

Also it excuses itself of this obligation, the treatment realized by entities without spirit of profit, whenever it refers specially to its collaborator members, depending on its purpose and providing that the data is not communicating to third without the assent of the data subject.

It is arranged that the treatments not automated of personal data can be notified eventually in a simplified form.

The notification will have to contain as minimum the following information:

"a) The name and address of the controller and of his representative, if any;
b) the purpose or purposes of the processing;
c) a description of the category or categories of data subject and of the data or categories of data relating to them;
d) the recipients or categories of recipient to whom the data might be disclosed;
e) proposed transfers of data to third countries;
f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures to ensure security of processing".

It is regulated the possibility that existence of previous controls for the beginning of those treatments that can suppose specific risks for the rights and freedoms of the data subject. These will be realized by the Supervisory Authority once it has notified it to the controller or processor who, in case of doubt, will have obligation of consultation.

Treatments are surrendered to advertising, and these will have to be guaranteed for the Members States. The Supervisory Authority will have to take a record of the treatments that have notified him and as minimum the following information will have to consist: name, direction of the controller or his representative and the transference of data planed to third countries.

In case of treatments not submitted to communication the controller binds to facilitate to everyone that requests it, at least information contained in the previous paragraph.

The exception to these obligations of notification are the records, which by virtue of legal or regulation dispositions, facilitate and are open to the public consultation, or to those that demonstrate a legitimate interest.

II.3. Judicial remedies, liability and sanctions.

4. The Directive 95/46/EC in the Chapter III (articles 22, 23 and 24) tries that the holders of the rights recognized by her are not defenceless before a violation of such, and for it he raises a regime of resources that to ours to understand is quite ample and flexible, admitting the possibility of interposing previous an administrative resource to the judicial one or contentious-administrative. In this point it would be possible to ask itself and it would be also optional the previous exposition of a judicial resource but in agreement with the literal tenor of article 24 of the Directive it does not seem to us permissible.

As far as the responsibility, the people who suffer a damage because of the illicit treatment of their personal character data will have right to demand to the people in charge the indemnification by the caused damages and damages. These could only be exempted partial or totally if they demonstrate that the caused damage is not imputable to them. In this point it enjoys great importance arranged in the Considering 55 when it arranges that "the damages that can undergo the people as a result of an illicit treatment have to be repaired by the person in charge of the data processing, which could only be exempted of responsibility if it demonstrates that is not to him imputable the detrimental fact, mainly if demonstrates the responsibility of interested or a case of greater force". The objective responsibility does not take shelter therefore of the people in charge of the damage, who do not only respond of the damage in any case but when they cannot prove that the fact cause of the damage is not attributable to them.

With respect to the sanctions, the article 24 marks that "The Members suitable States shall adopt measures to ensure the full implementation of the provisions of this Directive and shall in individual lay down the sanctions to be imposed in marries of infringement of the provisions adopted pursuant to this Directive". We appreciated as the communitarian norm is expressed in this point of very general form, letting to total freedom to the States Members to establish the measures and sanctions to adopt. He had been desirable to ours to understand the establishment of minimums that did not leave as much margin from decision to the communitarian countries at the time of determining them.

II.4. Transfer of personal data to third countries.

5.In the Chapter IV (articles 25 and 26) the Directive 95/46/EC are established some of the provisions concern the conditions under which personal data can be transferred to countries outside the EU. The application of these provisions has aroused interest and some concern among governments and

economic operators outside the EU and led to discussions between the Commission's services and government representatives from the US and other countries the EU.

At a time when an increasing quantity of personal data is processed and made available, the Directive 95/46/EC spells out the basic individual rights to privacy: for example, every person should have the right of access to personally identifiable data relating to him/her, and a right to rectification of those data where they are shown to be inaccurate. In certain situations, he/she should also be able to object to the processing of his/her personal data. In addition, individuals should be provided with information as to the purpose of processing and the identity of the data controller, so that they can exercise their right of access. Where "sensitive" data are involved (for instance, medical data, and data revealing racial or ethnic origin, religious or philosophical beliefs), additional safeguards should be in place, such as a requirement that the person concerned gives his/her consent for the processing.

At the same time, the Directive ensures that companies and other organisations will be able to transfer personal data throughout the EU. In most European countries, the protection of personal data is a constitutional principle, and the right to privacy is enshrined in the European Convention on Human Rights. Without the Directive 95/46/EC, different national approaches to data protection would create barriers within the market and the free movement of personal information would be impaired. In harmonising data protection laws, the Directive ensures the free movement of personal data within the EU.

On October 25th, 1998, the Directive 95/46/EC was due to be implemented into national law by all fifteen Member States. Irrespective of the national implementation measures, certain provisions of the Directive 95/46/EC will have direct effect in accordance with the case law of the European Court of Justice. The Directive 95/46/EC will apply throughout the EU, irrespective of whether the individuals concerned by the processing are EU citizens or not.

The Directive 95/46/EC establishes rules designed to ensure that data is only transferred to countries outside the EU when its continued protection is guaranteed or when certain specific exemptions apply. Without such rules, the high standards of data protection established by the Directive would quickly be undermined, given the ease with which data can be moved around on internationals networks.

The Directive 95/46/EC provides for the blocking of specific transfers where necessary, but this is a solution of last resort and there are several other ways of ensuring that data continues to be adequately protected while not causing disruption to international data flows and the commercial transactions with which they are often associated. All the same time, the Directive requires Member States to permit transfers of personal data only to countries outside the EU where there is adequate protection for such data, unless one of a limited number of specific exemptions applies. Where this is not the case, Member States must inform the Commission, which will start a Community procedure to ensure that any Member State decision to block a particular transfer is either extended to thee EU as a whole, or reversed. In this task, the Commission is assisted by a committee and a working party. The committee, set up by article 31 of the Directive 95/46/EC, is composed of Member State officials. Its particular task is to advise the Commission concerning decisions on transfers to third countries.

At the time, the article 25.4 of the Directive 95/46/EC foresees that decisions to block transfers are taken on specific individual cases, raised by a Member State. A decision to block a transfer would only apply to other transfers of the same type, not to all transfers to the country concerned. There is a general interest in keeping the scope of such decisions as narrow as possible. On the other hand, even where its found that there is not adequate protection, transfers may take place in circumstances specified in the article 26. This will be the case when, for example:

- The individual has given his unambiguous consent to the transfer, or
- The transfer is necessary for the performance of a contract with the individual concerned (for example, employment contracts) or the implementation of pre-contractual measures taken in response to his/her request (for example, application for a job), or

- The transfer is necessary or legally required for the establishment, exercise or defence of legal claims, or
- The transfer is necessary in order to protect the vital interests of the individual (for example, transfer of medical data concerning an individual hospitalised in a non-EU country).

Other exceptions are provided by the Directive 95/46/EC and show that, even for data flows to those countries, which do not ensure an adequate level of protection, there are a generous number of bridges and doors. For some of the doors, the key is held by the individual. However, another door remains open even where the above conditions are not met, and the keys of this door are held by industry itself.

6. In short, the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

The adequacy of the level of protection afforded by a third country shall assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations.

Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law in force in the third country in question and the professional rules and security measures which are complied with in that country.

Where the Commission finds that a third country does not ensure an adequate level of protection, Member States are required by the Directive to take measures necessary to prevent any transfer of data of the same type to the third country in question.

The Directive 95/46/EC also expresses the possibility that the Commission enters into negotiations with a view to remedying the aforementioned situation (for example, the case with US leading to the "safe harbor" negotiations with EU).

Transfers of personal data to a third country which does not ensure an adequate level of protection may take place on condition that one of the following conditions is met:
"a) The data subject has given his consent unambiguously to the proposed transfer;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

e) the transfer is necessary in order to protect the vital interests of the data subject;

f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case".

The Directive allows a Member State to authorise a transfer of personal data to a third country which does not ensure an adequate level of protection where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses. This possibility will, however, be closely surveyed by the Commission, which may object to it and compel the Member State to comply with such objection.

II.5. Codes of conduct.

7. In the Chapter V (article 27) the Directive 95/46/EC encourages that drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions.

The codes of conduct are "set of norms elaborated by a professional organism and that, without having binding power, has for purpose to organise and guide the attitude of companies" and the intention of the Directive 95/46/EC is promote the proper implementation of national provisions adopted by Member States.

Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes, which have been approved by the Working Party.

II.6. Supervisory authority and working party on the protection of individuals with regard to the processing of personal data.

8. The Chapter VI of the Directive 95/46/EC (articles 28, 29 and 30) establishes that the Members States will create independent Supervisory Authority of public character. These authorities will have to be consulted in case that the governments elaborate regulation or administrative measurements that affect the rights and freedoms of the persons in everything that one that refers to the treatment of his personal data. The Supervisory Authority will have the power of investigation necessary for the fulfilment of its mission of control; effective power of intervention, such us, to formulate reports before carrying out the treatments, and to guarantee a suitable publication of the above mentioned reports, or arranging the blockade, the suppression or the destruction of data, or even to prohibit provisionally or definitively a treatment, or directing a warning or admonition to the controller or of submitting the question to the parliaments or other political national institutions; procedural capacity in case of infractions to the national regulations or to put the above mentioned infractions in knowledge of the judicial authority.

As in any democratic state, the decisions of the Supervisory Authority will be capable of jurisdictional review. The Supervisory Authority will know about the requests that any person presents with regard to the protection of his rights, especially of the requests of monitoring of the legality of the treatment, and besides, the data subject will have right to be informed about the course that follows his request.

The Supervisory Authority will have to exercise the power that has been attributed of effective form and it will be able to be urged to exercising it for an Supervisory Authority of another Member State. Besides, these will have to cooperate between them in the necessary degree for the fulfilment of their functions, especially, interchanging that information which they consider useful.

The members and agents of the Supervisory Authority will be fastened, even after having stopped from their functions, to the duty of professional secret on confidential information to which they have had access.

Also the creation of a Working Party that will have consultative and independent character, and will be made up of a representative of the Supervisory Authority or authorities of each Member State, a representative of the Supervisory Authority or authorities created by the communitarian institutions and organisms, and by a representative of the Commission.

Each member of the Working Party will be designated by those that represent. The Working Party will make its decisions by simple majority from the representatives of the Supervisory Authority, and will choose its president, and its mandate will last of two renewable years.

The work of the Working Party will be the one of homogenize the application of the present Directive in the communitarian territory, to make opinions about the level of existing protection, to advise to the commission on any project of modification, in the scope of the present Directive, of the national legislation it would communicate to guarantee the rights and liberties of the physical people in which it concerns to the personal data processing and to issue rulings on the codes of conduct of communitarian level. Also, an annual report will be elaborated and published in which the protection level the physical people will be treated in which it concerns to the treatment of his data.

A committee made up of a representative of the Members States and presided over by the representative of the Commission will be created. Its mission will be to present an opinion on the projects of the measures that are going to be adopted and that could only be revoked acting the Council by qualified majority.

II.7. Community implementing measures.

9. The precision of the dispositions of the Directive 95/46/EC (Chapter VII- article 31) seems to exclude the necessity from measures of execution or application, since a priori it would be really difficult that some matter was not regulated by this one or by the national norms of transposition. But, what it happens with the data transfer to third countries, and if these are incapable to guarantee their protection. The answers to these questions we found them in article 25 of the Directive, who in her section 4 affirms “Where the Commission finds, to under the procedure provided for in article 31.2, that to third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this article, Member States shall take the measures necessary to prevent any to transfer of dates of the same type to the third country in question”. On the other hand section 6 continues saying that “The Commission may find, in accordance with the procedure referred to in article 31.2, that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this article, by reason of its domestic law or the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and

rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision".

The sight previously is amply just yet the inclusion in article 31 of the Directive 95/46/EC of communitarian measures of execution. The organ in charge to adopt them will be the Commission that will be attended by a Committee formed by representatives of the States members and presided over by a representative of this one. The Committee will issue a ruling on the project of the measures that are had to adopt displayed by the delegate of the Commission. This one will be the one in charge to adopt the opportune measures unless the same ones were not in agreement to the opinion of the Committee, in which case will have immediately to be, communicated the Council. In this case the Commission shall of defer application of the measures which it there are decided for to period of three months from the dates of communication and the Council, acting by to qualified majority, may take to different decision within the Time limit referred to in the first indent.

The Considering 66 anticipate that the execution measures are necessary with regards to the data transfer to third countries, and for it it's precise to attribute to the Commission execution competitions. Reason why we have seen previously, article 31 of the Directive 95/46/EC follows the guideline indicated by Considering with the specialties contained in the same one and that also we have mentioned, where it grants to the Council the power to revoke in certain cases the decisions of the Commission and to adopt others in his place.

III. Organic Law 15/1999 of 13 December on the Protection of Personal Data.

III.1. Principles of data protection.

10. The Organic Law 15/1999 of 13 December on the Protection of Personal Data is the result of the transposition of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such dates. And that as it could not be of another way, we did not find substantial differences with Directive 95/46/EC, although, is outlined the vocabulary and the expressions used for this way obtaining a greater legal rigor, because the Organic Law 15/1999 is not the original language in which the mentioned Directive wrote up itself, and the translations not always are made with the suitable rigor.

The law gathers its Title II and III, the principles relative to the protection of data and the rights of the people. Doing it, in the following way:

a) Data quality.
b) Rights of information in the collection of data.
c) Consent of the data subject.
d) Data specially protected.
e) Data relative to the health.
f) Security of the data.
g) Duty of secret.
h) Data communication.
i) Accesses to the data on behalf of third.
j) Contesting to valuations.
k) Right of consultation to the General Record of data protection.
l) Right of access.
m) Right of rectification and cancellation.
n) Procedure of opposition, access, rectification or cancellation

o) Tutelage of the rights.
p) Right of indemnification.

With regard to the data quality takes place a transposition that, as mentioned above, is almost literal in order to avoid the ambiguity in the language.

When we talk about the right of information to the data subject, we can see that the most important difference between the Directive and the Organic Law 15/1999 is the necessity of communication that demands in all the cases when it is transmitted the data to third, being irrelevant, that the transferor is an organization without spirit profit or no.

When we speak of the consent of the data subject, there is not an important relevance between the Directive 95/46/EC and the transposed law.

When we talk about the data specially protected, the Organic Law 15/1999 increases the guarantees of protection when it prohibits all those files that have as only purpose the storage of the data considered sensitive, that is to say, those that are referred to the sexual direction, union, political affiliation, etc. as well as, the consent has to be express and in writing.

The transposition that is made of the treatment of the data relative to the health is a literal copy of the gathered in Directive 95/46/EC.

In the case of the security, we found as main difference between the Directive 95/46/EC and the Organic Law 15/1999 that the last one does not consider the economic cost as a variable to consider at the time of establishing safety measures. Although, all this matter is held to further regulation development.

Duty of secret, it is widely gathered in the Organic Law 15/1999 not only it is applied, as the Directive does, solely to the referred data to the health and clinical files and the members and agents of the Supervisory Authority, but that extends all those people who take part in the data processing, and this obligation will even subsist after finishing their relation with the processor or controller.

Although at first sight, the data communication, can seem less strict in the national legislation, this is due to the existence of the dissociation process. This process makes that the identification of a person as a result of the viewing of its data is impossible. In addition, the Directive 95/46/EC is in charge mainly of the data transfer between States, whereas the Organic Law 15/1999 is more oriented to the internal traffic of them.

The Organic Law 15/1999 makes responsible to those persons to whom it indeed makes the treatment of the data, doing that this also consists in the contract which compulsory they have to sign the controller and the processor.

The article 13 Organic Law 15/1999, as Directive 95/46/EC does, establishes the right to not be submitted to a decision with legal effects based on a data processing that evaluates their personality. Being solely possible this kind of treatments when it is in benefit of the data subject.

The right of consultation to the General Record of Data Protection is formed in the same way that Directive 95/46/EC, with the reservation that in the Spanish legislation this consultation will be free.

The access right, stays formed as a gratuitous right, that will be able to be exerted in non inferior periods to twelve months, except in the cases in which the data subject credits a legitimate interest, in which case could be exercised prior to the fulfillment of the period before mentioned.

The right of rectification or cancellation comes formed as obligation of the controller that in addition will have to make it in a term of ten days. The rectification or cancellation will be carried out when treatment does not adjust to the arranged thing in the law and individual when the data are inexact. Moreover, these data will stay blocked and to disposition of the public administrations judges and courts. The rectifications or cancellations that took place will have of being communicated all to those people to whom the data have been yielded them.

On the other hand, and connected with the right of a opposition, access, rectification or cancellation, we were whereupon the procedure to exert these rights will settle down of regulation development, and whose only legal requirement is to be free.

The protection of rights that attend the data subject will be demanded before the Data Protection Agency. The Agency will have to solve of express form in a maximum term of six months, and against these resolutions contentious-administrative resource will come.

With reference to the right to indemnification to that they have right data subject, as a result of the breach of the arranged thing in Organic Law 15/1999, it will depend on the ownership of the file, if this it is of public ownership follows the contentious-administrative way, on the contrary if the file is of private ownership the action will be exercised before the ordinary jurisdiction.

III.2. Public and private files.

11. The personal character data can be gathered in public or private files. Title IV of Organic Law 15/1999 gathers this distinction and gives different regulation according to are in one or another one, differentiation that we thought.

III.2.1. Public files.

For its creation, modification or extinction is necessary published legal disposition in the corresponding official Newspaper. It is allowed not even with general character that the data gathered or processed by the public Administrations for the performance of their functions communicate to others for the exercise of different competitions or that they treat on different matters, although it anticipates the disposition of creation of file or one of superior rank (Sentence 290/2000 of the Spanish Constitutional Court). This decision seems guessed right, because in opposite case it would equip the Administrations with an almost absolute liberty to transfer among them of limitless form the personal character data that own Organic Law 15/1999 protects. Despite an exception exists: this communication is allowed when this one intends the later treatment of the data with historical aims, statistical or scientific. Within the files public are those created by the Forces and Bodies of Security of the State that contain personal character data, that by to have gathered for administrative aims, must be object of permanent registry. Logically one allows to the collection and treatment for police aims of these data by the Forces of Security without consent of the people affected in determined exceptional assumptions: when it is necessary for the prevention of a real danger for the public security or the repression of the penal infractions.

The Organic Law 15/1999 gathers throughout his articulated all a series of opposable rights by interested nobody whose personal character data are put under treatment as much in files public as prevailed (straight of access, cancellation, etc.). Although in principle and as it regulates general is not possible to restrict the exercise of these rights, a chain of exceptions in the articles 23 and 24 exists that in any case that seems we must consider them like appraised cases. Outside these it does not seem

reasonable to exception the exercise of these rights, because in opposite case we would be possibly before a situation of defencelessness of the affected ones.

III.2.1. Private files.

The creation of these files by person, company or private organization is subject to a series of consisting of formalities the respect of the guarantees that the Organic Law 15/1999 establishes for the protection of the people and the previous notification to the Agency of Protection of Data.

The practice of certain companies or organizations to deal with the personal character data with aims is very well known about publicity and commercial prospecting without having an express consent of the interested ones. In order to avoid the violation of the rights of these that use names, directions or other personal character data for publicity, remote sale and other analogous activities, must count on the consent of the interested ones, them to have obtained with the consent of these, or that appear in accessible sources the public. In addition it is recognized affected in these cases exercise of the rights of access and opposition (if the data come from sources of accessible to the public also confers a information right to them). On the other hand the possibility that fits these same companies ask for to the organisms competent public a copy of the promotional census (where names, last names and directions contained in the electoral roll consist) for the period of use of a year. If the interested ones do not wish to appear in this one it they can solicit through the procedures that according to the Organic Law 15/1999 "they will be regulated lawfully". This remission to the prescribed activity, frequents throughout all the articulated one, supposes a content emptiness that can put in danger the defence of the rights of the affected ones, reason why had been desirable that the Organic Law 15/1999 regulated the applicable procedures.

As far as the possibility of creation of codes type by means of agreements of the people in charge of files deprived public and that establishes applicable procedures, analogous or similar regime of organization, and other conditions, it is allowed whenever they respect the content of the Organic Law 15/1999 and its norms of development.

III.3. International movement of data.

12. In the article 33 of Organic Law 15/1999 establish that there may be no temporary or permanent transfers of personals data which have been processed or which were collected for the purpose of such processing to countries which do not provide a level of protection comparable to that provided by the Organic Law 15/1999, except where, in addition to complying with the Organic Law 15/1999, prior authorisation is obtained from the Director of the data Protection Agency, who may grant it only if adequate guarantees are obtained.

The adequacy of the level of protection afforded by the country of destination shall be assessed by the Data Protection Agency in the light of all the circumstances surrounding the data transfer or category of data transfer. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question, the content of the reports by the Commission of the EU, and the professional rules and security measures in force in those countries.

But the provisions of the article 33 of the Organic Law 15/1999 shall not apply where:

“a) The international transfer of personal data is the result of applying or agreements to which Spain is a party.

b) The transfer serves the purposes of offering or requesting international aid.

c) The transfer is necessary for medical prevention or diagnosis, the provision of health aid or medical treatment, or the management of health services.

d) Where the transfer of data is related to money transfer in accordance with the relevant legislation.

e) The data subject has given his unambiguous consent to the proposed transfer.

f) The transfer is necessary for the performance of a contract between the data subject and the controller or the adoption of precontractual measures taken at the data subject’s request.

g) The transfer is necessary for the conclusion or performance of a contract concluded, or to be concluded, in the interest of the data subject, between the controller and a third party.

h) the transfer is necessary or legally required to safeguard a public interest. A transfer requested by a tax or customs authority for the performance of its task shall be considered as meeting this condition.

i) The transfer is necessary for the recognition, exercise or defence of a right in legal proceedings.

j) The transfer takes place at the request of a person with a legitimate interest, from a public register, and the request complies with the purpose of the register.

k) The transfer takes place to a Member State of the European Union or to a country which the Commission of the European Communities, in the exercise of its powers, has declared to ensure an adequate level of protection”.

III.4. Data Protection Agency.

13. So and as it arranges Directive 95/46/EC, the Members States will create control authorities, and that this mandate comes developed in the Title VI under the name "Agencia de Protección de Datos".

Its an Institution of Public Right, with own legal personality and total public and private capacity. It acts with total independence of the Public Administrations in the exercise of its functions.

The Agency is made up, in addition to a body of officials government, the organs that come regulated in the Organic Law 15/1999, this are: the Director, the Consultative Council and the General Record of Data Protection

The position of Director of the Agency lasts of four years, and their main functions are the direction and that to touch the representation of the same one. These functions will exert them independently and objectivity and will not be subject to instruction some, will have solely to listen to the Consultative Council in those proposals that this one makes in the exercise of its functions.

The Consultative Council is an advisory organ of the Director of the Data Protection Agency, and will be made up of the following members:

a) A Deputy, proposed by the Congress of the Deputies.
b) A Senator, proposed by the Senate.
c) A representative of the Central Administration, designated by the Government.
d) A representative of the Local Administration, proposed by the Spanish Federation of Municipalities and Provinces.
e) A member of the Royal Academy of History, proposed by the same one.
f) An expert in the matter, proposed by the Superior Council of Universities.
g) A representative of the users and consumers, selected of the way that is regulation prescribed.
h) A representative of each Community that has created a Data Protection Agency in its territorial scope, proposed in agreement with the procedure that establishes the respective Autonomous Community.
i) A representative of the sector of private files, for whose proposal the procedure will be followed that is regulated prescribed.

The functions of the Data Protection Agency, come collections in article 37 of the Organic Law 15/1999 that continuation we reproduce:

"a) To guard by the fulfilment of the legislation on data protection and to control its application, in special with respect to the rights of information, access, rectification, opposition and cancellation of data.
b) To give the authorizations anticipated in the Law or its regulation
c) To dictate, in its case, and without damage of the competitions of other organs, the instructions precise to adapt the treatments to the principles of the present Law.
d) To fulfil the requests and claims formulated by the data subject.
e) To provide information to the people about its rights in the matter of treatment of personal data.
f) Require to the controller and the processor, previous hearing of these, the adoption of the necessary measures for the adjustment of the data processing to the dispositions of this Law and, in its case, to order the cessation of the treatments and the cancellation of the files, when one does not adjust to its dispositions.
g) Exercise the sanctioning power in the terms anticipated by Title VII of the present Law.
h) To inform, with mandatory character, the projects of general dispositions that develop this Law.
i) To obtain of the people in charge of the files whichever aid and information considers necessary for the performance of its functions.
j) To ensure the publicity of the existence of the files of personal data, whose effect will periodically publish a relation of these files with the additional information that the Director of the Agency determines.
k) To write an annual memory and to send it to the Ministry of Justice.
l) Exercise the control and to adopt the authorizations that come in relation to the international movements of data, as well as to perform the functions of international cooperation in the matter of protection of personal data.
m) To ensure the fulfilment of the dispositions that the Law of Public Statistical Function establishes with respect to the collection of statistical data and to the statistical secret, as well as to give the precise instructions, to consider on the conditions of security of the files constituted with exclusively statistical aims and for exerting the power to which article 46 talks about.
n) Whichever others are attributed to him by legal or regulation norms".

The General Record Data Protection of has like main function the inscription of the files, as much of public as private ownership, the authorizations that must grant the Data Protection Agency, the codes type and the data relative to the files and that is necessary for the exercise of the rights of information, access, rectification, cancellation and opposition. All these functions will be developed by regulation way.

The Organic Law 15/99 becomes echo of the had thing in Directive 95/46 and granted the protection agency data the inspection power, investing of public authority to the civil employees who make these functions.

As it corresponds to the territorial organization of the State, the Autonomous Communities will have the power for the creation of . Supervisory Authorities that, subordinated to the Data Protection Agency, guarded by the safeguard of the rights of the data subjects in those files that they have as it bases exclusive competitions of the Autonomous Communities. Also, the Autonomous Communities will be able to maintain files that are based on their exclusive competitions.

III.5. Infringements and sanctions.

14. The infractions that the people in charge of the files and the ones in charge of the treatments can commit will have to be described like slight, serious or very serious, habitual typology when the administration acts by means of its sanctioning power. The list of punishable actions or omissions contained in the article 44 is quite ample although no exhaustive, and goes from not taking care of by formal reasons the request for interested of rectification or the cancellation of the personal data gathered in a file when it comes legally, to the collection of these by means of fraud or deceit. We do not think that the enumeration contained in this article is exact and does not include any other infraction committed by the previous subjects that harm the rights of the holders of the data contained in their registries and that are protected by Organic Law 15/1999. The opposite would suppose a severe unprotected of the affected ones.

With respect to the sanctions by the infractions committed by the ones in charge and people in charge of the files, they are of pecuniary character (with some exception as we will see more ahead), and logically the quantity of the sanction will go increased based on the gravity of the action or committed omission (slight infraction, burdens or very serious). To its concrete concretion, section 4 of article 45 has a series circumstances to value, such as the benefits obtained by the caused violators or damages and damages, that despite we considered does not suppose *numerus clausus* in accordance of as it finishes "to any other circumstance that is excellent to determine the degree of present unlawfulness and culpability in the concrete performance offender". In this point we emphasized the disproportionally of the economic sanctions, that due to the impetus of the Spanish Government to punish very severely the infractions in this matter has located to Spain like the country "with the sanctioning regime more hard of all the European Union".

When the violators responsible or are ordered of files public, the Director of the Agency of Protection of Data will be able to carry out a series of tending performances to obtain the adoption of all the measures necessary to stop the effects of the infraction (even the immobilization of very serious files in cases, applicable also to those of private ownership) and the initiation of disciplinary measures in his case (to remind that he is workers to the service of the Administration). This supposes that the sanctioned violator a pecuniary sanction will not be dominated to him obligatorily, unlike the sanctioning regime applicable to the violators responsible for private files where always she will be pecuniary.

As far as the sanctioning procedure, article 48 anticipates its establishment by prescribed route, disposition that the dangerous tonic general of the Organic Law 15/1999 follows which since already we have indicated previously, it can be dangerous and suppose a violation of the rights of the affected ones.

IV. German Data Protection in the World Wide Web.

IV.1.Introduction.

15. The digital revolution and the rise of the Internet have opened up important new ways for people to obtain information, interact and do business with each other. Consumers can now research and compare products and make purchases from their home, obtaining far more information more quickly than they could ever before. But these same technologies have reduced the costs of gathering, storing, manipulating and transmitting information of all kinds, especially information relating to the commercial behaviour of consumers. Neither the collection of such information nor its use to facilitate targeted marketing and relating practices is new. Enormous amounts of data have long been available offline, such as warranty cards, and many other traditional methods. What the digital revolution has done is increasing the efficiency, amount and effectiveness with which such information can be collected and used.

In order to create personalized websites and to offer tailor-made products and services for the needs of consumers, tele-and mediaservices use means such as cookies, CGI-script, Java and Javascript, web bugs, bookmarks, web-tracking, permission marketing, customer relationship marketing and many others. Consumers clearly are concerned about information collection by commercial web sites. Therefore, the success of a current tele-or mediaservice depends upon whether the web surfer trusts the companies' privacy policy. Additionally, the German law sets a limit to the collection of consumer's data through a variety of provisions: basically the Federal Data Protection Act (BDSG), the Teleservices Data Protection Act (TDDSG) and the Interstate Data Protection Agreement (MDStV). The constitutional roots of these acts lie in the general right of personality which was granted the first time in the famous census judgement. It ensured that every citizen can decide about the surrender and use of it's data.

IV.2. Principles of Data Protection.

16. For applying the right act, one has to divide between tele- and mediaservices. Teleservices are electronic information- and communication services, which are meant for individual use, for example, access provider, electronic banking, databases, e-commerce and other services with individual aspects. They are under the federal competency according to article 73 BDSG, thus the Teleservices Data Protection Act applies to these services. Mediaservices are aimed for the general public; for example, online-newspapers, online-magazines, online-presentations of companies and editorial newsletters. The federal states have the competency over the mediaservices, article 75.2 BDSG, and the Interstate Data Protection Agreement must be applied. Many online services are both teleservices and mediaservices, such as Yahoo, which offers news, e-commerce and e-mail services. In that case both acts can be applied depending on the problem. But a differentiation between these two acts is unproblematic because the provisions have almost the identical wording. Therefore, I want to focus this essay predominantly on the teleservices and thus the TDDSG. I will not look at the sole transport level (for example, e-mail transport and internet telephoning) and the data processing relating to the bank and insurance business. The general provisions for data protection of the BDSG must be applied if the specialized acts such as the TDDSG do not provide a particular provision.

IV.3. EU-Directive.

17. In order to remove the obstacles to the free movement of data without diminishing the protection of personal data, the directive 95/46/EC was developed to harmonize national provisions in

this field. As a result, the personal data of all citizens have an equivalent protection across the EU now. But even before Germany transformed the directive into federal law (through an amendment of the BDSG) there already existed the BDSG with a high standard of data protection. The TDDSG was the first legislation in Europe specifically to address privacy and data protection issues in an Internet context and was passed as one element of a broader legislative package (the IuKDG) in 1997 and was the last time amended by article 3 of the bill on legal framework conditions for electronic commerce "EGG" in 2001. The Interstate Data Protection Agreement entered into force in the same year as the TDDSG, in 1997.

IV.3.1. Types of Data.

18. One must distinguish four types of data, which can be used for profiles: a) *Contractual data*, s 5 TDDSG, are personal data which are vital for the foundation, content or alteration of a contract and for the use of a Teleservice; for example, name, address, IP-number, e-mail address, date of birth, user ID, number of the credit card and others; and, b) *Utilization data,* are basically data, which enable the user to utilize teleservices and to charge the user for the use of teleservices. Utilization data include in particular characteristics that identify the user, information on the beginning, end, and extent of each use and information on the teleservices (clickstream) accessed by the user according to s 6 I a,b,c TDDSG. It is questionable whether personal data with content (e.g. content of an e-mail or of a guestbook or a chat room), which are transferred through the use of teleservices, are covered by the TDDSG or the BDSG. The courts and the legal literature have not found a satisfying answer yet. These types of data are all powerful sources for teleservices because they reveal the consumer behaviour, interests, and activities of the user. In order to prevent teleservices to create unwanted profiles of its' users the TDDSG and the MDStV impose special duties on tele- and mediaservices.

IV.3.2. Legal Requirements for Tele- and Media Services.

1. Information of the User.

19. The provider has to inform the user prior to the beginning of the procedure about the type, scope and purpose of the collection, processing and use of personal data according to s 4 I TDDSG and s 12 VI MDStV. To the obligation of informing the user belongs also the notification of the user's right to withdraw his consent (prior to the user's declaration of consent), s 4 III TDDSG, and the information of the user about his right of objection relating to the compilation of pseudonym-based use-profiles for purposes of advertising, market research, and structuring the tele- and mediaservices to comply with demand under s 6 III TDDSG and s 13 IV MDStV. Many companies have noticed that data protection is a way to achieve confidence in the users' minds and therefore, have integrated these duties in their privacy policy about which the Internet surfer is informed prior to the beginning of the procedure. The collection of personal data starts basically when a homepage is entered, because the IP address and other technical data of the user are transferred automatically to the provider. At least at the moment when the user is asked to give personal data or when files with direct or indirect connection to personal data, which are stored at the computer, are collected (for example, cookies) the provider must inform the user. When the data of the user are processed outside the EU, the provider shall inform the user as well under s 4 I TDDSG. This can be achieved by an explicit link to electronic form or a pop-up window. Additionally, the provider has to ensure that the content of such information is accessible to the user at any time in accordance with s 4 I TDDSG.

2. Cookies.

20. Cookies are pieces of information generated by a web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information. Originally they were implemented to allow user side customisation of web information, e.g. cookies were/are used to personalise web search engines and to store shopping lists of items a user has selected while surfing through an online shop. Normally cookies make use of user specific information transmitted by the web server into the user's computer. Web servers automatically gain access to relevant cookies whenever the user establishes a connection to them, usually in the form of web requests. The duty of information concerns cookies, which are stored for a longer time at the user's computer. The duty to inform the user does not arise when personal data are automatically erased or blocked upon the conclusion of the procedure according to s 4 IV Nr. 2 TDDSG. Personal data means any information concerning the personal or material circumstances of an identified or identifiable individual under s 3 I BDSG. In case of an objection, s 6 III TDDSG, the provider is not allowed to store cookies, which are meant to compile pseudonym-based use profiles.

3. Principle of Data Reduction and Data Economy.

21. The principle of data reduction and data economy as a basic principle of data protection, can be found therefore in s 3 a of the BDSG and provides that the tele- and mediaservice provider has to design and select his data processing systems in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. This principle applies to Tele- and Mediaservices if they can make a connection with special knowledge (for example, if they offer e-mail services, they can make a connection through Log-In) from their collected data to a particular person.

a) Anonymous and Pseudonym Possibilities of Use.

One aspect of the principle of data reduction and data economy is the duty of the provider to make it possible for the user to utilize and pay for teleservices/mediaservices anonymously or under a pseudonym if this is technically possible and can be accomplished at reasonable effort under s 4 VI TDDSG, s 13 I MDStV. The new s 3 VI a BDSG supplies us with a definition of aliasing: it "means replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject". A pseudonym can be the dynamic IP-Address, a user-ID (Login) or an electronic signature by a trustworthy third party (certification service). Everyone can let a certification service certify a signature key which identifies him not under his real name but under a fictitious name in accordance with s 7 I Nr. 1 SigG.

b) Technical and Organizational Measures.

Another aspect of the principle of data reduction and data economy can be found in s 4 IV TDDSG. This section imposes the duty on the provider to take technical and organizational measures to ensure that the user can break off the connection at any time and that the personal data can be erased or blocked immediately upon conclusion of the procedure. This can be the case when erasure is prohibited by legal statutes -such as through s 257 HGB the provider can be forced keeping the contractual and utilization data for 10 years. An additional important measure which has to be ensured is the provision

that personal data, which relate to the use of several teleservices by one user, may be processed separately. The last important measure aims to prevent especially the formation of profiles because user profiles pursuant to s 6 III TDDSG may not be combined with data on the bearer of a pseudonym. Especially the last measure was integrated into the TDDSG due to Art. 17 of the EU-directive for data protection.

4. Consent.

22. The principle rule states that personal data may only be collected, processed and used by providers for performing teleservices/mediaservices if permitted by a regulation or if the user has given his/her consent under s 3 I TDDSG or s 12 II MDStV. The provider is not allowed to make the rendering of teleservices/mediaservices contingent upon the consent of the user to the processing or utilization of his data for other purposes, s 3 IV TDDSG, s 12 IV MDStV. The consent can be demanded if other access to these services is provided to the user.
Therefore, with consent of the user it is permissible:

a) To collect, process and utilize personal contractual and utilization data for purposes of consulting, advertising, market research and structuring the services to comply with demand of the user, s 5, 6 I TDDSG and s 14 II MDStV.

b)To collect the e-mail address for a newsletter

c)To collect particular interests in order to tailor-made the offer of tele/mediaservices.

The provider can offer the user the possibility of declaring his consent electronically. In that case the provider must guarantee that the consent can be given by the user only through unambiguous and deliberate act, such consent is recorded and the text of such consent can be accessed at any time by the user according to s 3 III in connection with s 4 II TDDSG; s 12 VIII MDStV. Thus a mouse click on a prepared electronic declaration is sufficient for a valid consent. It must be emphasized that the electronically consent does not relate to s 126a BGB where a qualified electronic signature is required.

A consent can be given as well in form of a contract between the provider and the user where the user declares the renunciation of his right to withdraw his consent at any time in the future for a certain amount of money. The provider should convince a user of the fair and lawful use of his personal data. This can be achieved through a privacy statement on the website which provides all the information the user needs and the law stipulates. A good example of a privacy policy provides the company Nestle and can be found in the appendix.

4. Data Subject's Right of Access.

23. The user has the right that the tele- or mediaservice provides information on data stored on the user or on his pseudonym immediately upon request under s 4 VII TDDSG, s 16 I, III MDStV. The information can be provided electronically. The data subject's right of access corresponds to the obligation of the provider to inform the user prior to the beginning of the procedure, about the type, scope and purpose of the collection, processing and use of his personal data, because without the knowledge that the provider collects personal data it would not be possible to request the information on data stored on the user by the provider.

This obligation can be realized through an online information after identification of the user through entering a password or through an electronic message at the user's e-mail address.

One of the inalienable rights of the data subject is the right of access. It cannot be excluded or restricted by a legal transaction under s 6 I BDSG. Therefore, a user's right to access cannot be excluded or restricted through a contract between the provider and the user.

5. Extern Links

By means of links many informations and offers in the web can be tied together. It can be a disadvantage for the user when he leaves the area/web page of a certain tele- mediaservice without knowing it actually. This other provider may have a totally different or even no privacy policy. Moreover, there is often a high dovetailing between information and advertisements in the Internet, which can be very irritating for the user. Technically possible is also an automatically re-forwarding to another provider by means of an inline link.

In order to protect the user it is necessary to notify the user in case of any re-forwarding to another provider, s 4 V TDDSG, s 13 III MDStV. This provision applies also to advertisement in the net, which normally re-forwards a user (through a link) to another provider. Inline links where the user cannot recognize that he was led to another web page are therefore as well unlawful. As an additional protection s 7 TDG provides that providers of commercial communications (e.g. advertisement in the internet), which are part of, or constitute a teleservice shall ensure that commercial communication is clearly recognizable as such and the natural or legal person on whose behalf commercial communications is transmitted is clearly identifiable.

Without provisions of that kind, the user could neither make use of his right of access nor could a control of data protection take place.

IV.4. Infringements and Sanctions.

24. We can distinguish between administrative offences and criminal offences.

IV.4.1. Administrative Offences.

The Section 9 of the TDDSG, which regulates the consequences of an administrative offence, was integrated during the last amendment. The reason behind this integration was the prevention of disadvantages for the competition of companies, which acted in accordance with the TDDSG. Furthermore, another reason was the enforceability of data protection according to teleservices.

Under s 9 I TDDSG an administrative offence shall be intentional or negligent if offering of a teleservice made contingent on the consent of a user to the processing or utilization of his data for other purposes in violation of s 3 IV TDDSG (Nr. 1), in violation of s 4 I sentence 1 or 2 TDDSG (Nr. 2) if the provider fails to inform the user and fails to inform fully and timely, if the provider fails to comply or to comply fully with one of the duties to ensure of s 4 II, IV sentence 1 Nr. 1 to 5 TDDSG (Nr. 3), if the provider collects, processes, utilizes personal data, or fails to delete personal data or deletes it completely in violation of s 5 sentence 1 or s 6 I sentence 1, VIII sentence 1 or 2 (Nr. 4) and finally, if the provider combines a user profile with data on the bearer of a pseudonym, in violation of s 6 III sentence 3 TDDSG.

An administrative offence as mentioned above can be punished by monetary fine not to exceed 50 000.- Euro under s 9 II TDDSG. Whereas an administrative offence which violates certain sections of the BDSG can be punished by monetary fine from 50 000 to 250 000 Euro under s 43 III BDSG. Now the question arises why the fine in the TDDSG is that low compared to the fine in the BDSG. The enormous high economic power of some teleservices was not taken into consideration sufficiently. Therefore, the amount of the fine is not deterrent enough for big teleservice companies in the Internet.

For the same reasons as mentioned above in s 9 I TDDSG can a mediaservice be punished by a monetary fine not to exceed 250 000 Euro under s 20 II MDStV. This discrepancy between the amounts of fines should be brought into line by raising the fine for an administrative offence of teleservices in s 9 II TDDSG to 250 000 Euro in order to prevent a discrimination of the mediaservices and to ensure a higher protection of the user in the electronic commerce.

IV.4.2. Criminal Offences.

There is no section in the TDDSG or the MDStV, which regulates whether a violation of one of the sections represents a criminal offence. Whereas s 44 I BDSG states that anyone who wilfully commits an offence specified in s 43 II BDSG in exchange for payment or with the intention of enriching himself or another person or of harming another person shall be liable to imprisonment for up to two years or to fine. Before the TDDSG and the MDStV entered into force in the year 1997, s 44 BDSG (which regulates the criminal offence) was also applied to tele- and mediaservices. The general rule states that the provisions for data protection of the BDSG must be applied if the specialized acts such as the TDDSG do not provide a particular provision. This would lead to the conclusion that s 44 BDSG must be applied to tele- and mediaservices. But the application is not that easy or almost impossible, because offences specified in s 43 II BDSG –which represent also a criminal offence according to 44 I BDSG- are not totally transferable to the provisions of an administrative offence under s 9 I TDDSG and s 20 II MDStV.

For the aim of legal security the legislator should therefore react and solve this issue through an amendment of the TDDSG and the MDStV by inserting a new section for criminal offences.

V. Final conclusions.

25. As it indicates to the Organic Law 15/1999, personal character data can be gathered in files public or prevailed. Act 15/1999 offers an ample regulation in this matter like we have seen, treating from the requirements to create, to modify or to extinguish the registries, to the rights that in this subject have the people whose personal character data are contents in these files. Despite the complete treatment that the Act offers, we have been able to verify that she is not free of critics. Thus we do not understand the different regulation that public gives between the files and the private ones, nor dangerous. remission from the regulation of certain aspects by prescribed route.

26. The regime of punishables infractions committed by the ones in charge of the different files from contained personal character data in Organic Law 15/1999, in spite of being very ample, we do not have to describe it like exact: any other infraction committed by the previous subjects that harm the rights of the holders of these data will be sanctionable. If in this one subject the Organic Law 15/1999 offers a complete regulation and very guessed right, in the treatment of the sanctions we cannot say the same. The disproportionality of the economic sanctions (only the existing ones except for rare exception) is the greater black point in this point. As far as the sanctioning procedure, one anticipates

his establishment by prescribed route, resource that since already we have declared in numerous occasions can be dangerous.

27. The regime of resources, responsibility and sanctions proposed by the Directive 95/46/EC is frankly guessed right. With respect to the resources, we have seen as the communitarian norm is very flexible, containing one more a regulation than sufficient to such protect the interests of the holders of personal character data gathered in files before a possible violation of by the ones in charge or people in charge of these. These also assume the responsibility respect to the caused damages to these holders by the illicit treatment of their data if they are to them imputable. Despite the Directive 95/46/EC it does not gather the objective responsibility, which seems to us reasonable since it would not just turn out nor originating to make responsible to the ones in charge of the files by damages caused because of the own holder of the personal character data or by greater force. As far as the sanctions, the arranged thing by the Directive 95/46/EC is too general, letting almost total freedom to us to the States to legislate on this subject, with the dangers that this can generate.

28. One of the greater successes of the Directive 95/46/EC under our point of view has been the inclusion in her of execution measures. Its importance is, like we have seen, in the guarantees that the norm for the case that establishes personal character data of people contained in a file of any State are transferred member to third countries (incapable sometimes to guarantee its protection). Therefore the importance of the inclusion of article 31 of the Directive 95/46/EC is beyond all doubt, no matter how much we could think in principle that the precision of the dispositions of the communitarian text and the fact of its later transposition by the States Members would exclude the necessity to regulate such community execution measures.

29. In other hand, to sum it all up, Germany has a high standard of data protection in the Internet and the user could calm down. The rules in the TDDSG and the MDStV are largely based on the core principles of fair information practices found in the BDSG and in the constitutional roots of data protection. What is innovative about the Acts, though, is the way in which they extend theses principles to cover a variety of issues – transactional anonymity, pseudonymity, cookies, processing of clickstream data, etc., which have gained prominence with the emergence and widening use of the Internet.

30. The remaining task for the government and the tele- and mediaservices is to spread the fact of the high standard of data protection in Germany and the EU among the Internet users. Given that they succeed in achieving this aim e-privacy/data protection in the Internet won't be a hindrance for a booming e-commerce anymore.

Bibliography..

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., "Notas a la nueva regulación de la protección de datos de carácter personal" en *LA LEY*, núm. 5036, 17 de abril de 2000.

AMADEO GADEA, Santiago Luis, *Informática y Nuevas Tecnologías*, La Ley-Actualidad, Madrid, 2001.

APARICIO SALOM, Javier, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi Editorial, Elcano (Navarra), 2000.

ARRIBAS LUQUE, J. M., "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: el sistema de principios de puerto seguro" en *LA LEY*, núm. 5497, 7 de marzo de 2002.

BECK'SCHER IUKDG COMENTAR. *Informations- und Kommunikationsdienstegesetz, 1.* Auflage, München 2001.

DE MIGUEL ASENSIO, P., *Derecho privado de Internet*, Civitas, Madrid, 2000.

ESTEVE GONZÁLEZ, Lidia (coord.) y otros, *Derecho e Internet. Textos Jurídicos Básicos*, Editorial Compás, Alicante, 2001.

FERNÁNDEZ SAMANIEGO, Javier, "España: La nueva Ley de Protección de Datos de Carácter Personal española" en *Revista Electrónica de Derecho Informático (REDI)*, 2002.

GARCÍA MESEGUER, Mª. D. y MEDRÁN VIOQUE, R., "La protección de datos de las personas en el tratamiento de datos: Principios y Derechos. Breve comentario de la transposición de la Directiva 95/46/CE a la Ley Orgánica 15/99" en *Revista electrónica V-lex*, 2002.

HEREDERO HIGUERAS, M., *La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal*, Tecnos, Madrid, 1996.

HEREDERO HIGUERAS, M., *La Directiva Comunitaria de protección de los datos de carácter personal*, Editorial Aranzadi, Pamplona,1997.

HERRÁN, A., *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999.

LAPP, THOMAS. Cookies: *Monster oder harmlose Kekse,* in IT- Rechtsberater 5/2001, S. 113-115.

MANRESA FARRERAS, B., "Los datos personales en la legislación en materia de protección de datos: ¿Qué debe entenderse por dato de carácter personal? en *Revista Electrónica de Derecho Informático (R.E.D.I.)*, núm. 45, 16 de marzo de 2002.

MARZO, A., "Novedades de la Ley de Protección de Datos" en *Revista IURIS*, Madrid, 2002.

NESTLE (Homepage) http://www.nestle.com/html/privacy.html

RASMUSSEN, HEIKE. *Datenschutz im Internet, in Computer* und Recht 1/2002, S. 36-45.

ROCA JUNYENT, M. Y TORRALBA MENDIOLA, E., "Ley de Protección de datos" en *LA LEY*, núm. 5014, 16 de marzo de 2000.

SCHMITZ, PETER *TDDSG und das Recht auf informationelle Selbstbestimmung,* 1. Auflage, München 2000.

SCHUSTER/MÜLLER/DREWES *Datenschutz und Sicherheit im Internet,* in Multi-media und Recht Beilage 3/2002, S.37-41.