[HS06] Jan Hansen, Katharian Selmeczi; Legal Chances and Restrictions in International Research Projects. New Advances in Multimedia Security, Biometrics, Watermarking and Cultural Aspects. Logos Verlag, Berlin, Oktober 2006, S. 135-160

Legal Chances and Restrictions in International Research Projects

JAN HANSEN, KATHARINA SELMECZI

Contents

1 Copyright 136
1.1 General Provisions 136
.2 European Community 138
1.3 National Law Systems Germany, Italy, India 141
2 Data Protection 144
2.1 General Provisions 144
2.2 European Community 145
2.3 Germany 146
2.4 Italy 148
2.5 India 148
3 Probative Force of Electronic Documents 149
3.1 General Provisions 149
3.2 European Community 150
3.3 Germany 152
3.4 Italy . . . . .
3.5 India 155
4 Virtual Presence in International University Examinations 156
4.1 General Provisions 156
4.2 Germany 157
4.3 Italy 158
4.4 India 158
5 Acknowledgement 159

Abstract

The workpackage "Legal Aspects of DRM and Biometrics" provides basic information about copyright, data protection and probative force of electronic documents.

1 Copyright

1.1 General Provisions

Copyright is a part of the big field of Intellectual Property. Intellectual Property protects two main types of intellectual creations.

One main type is Industrial Property with different kinds of special sections. Under Patent all kinds of new technical inventions are protected after a formalised registration procedure. Patents on compurter-programms are intensly discussed at the moment, for example; if business processes should be patentable and if there should be patents on trivial software solutions. Trademark means all kind of signs, word-combinations and symbols used for identification in commerce, so that the origin of goods or services can be distinguished. The second main type of intellectual property is Literary and Artistic Property, this covers novels, drama, film, and the Fine Arts. Here we find copyright law [Adr03].

Copyright law has to balance a fundamental conflict. We find a legal expression of this conflict in the Declaration of the Human Rights which was passed by the United Nations in 1948:

Art. 27 (1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits. (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

These ideas have international acceptance, many countries agree to them. But how are these abstract ideas transported into daily life? They go through several steps of concretion. The first step to give life to these ideas was the conclusion of international multilateral treaties. One of the first and most important of these treaties is the Berne Convention. It was founded in 1886; in 1998 there were 157 member states. In order to this treaty, the members agree on basic standards for the protection of literary and artistic works. Each member state agreed to form their national law system in accordance to the convention. Participating countries give up a part of their identity to cope with the provisions of other nations. That can only work, if the convention describes at least a common denominator. Here we can find the General Provisions of copyright which guarantee a wide range of protection. Productions in the Scientific Domain are protected too, this covers also computer programms, printed and acoustic learning material and - as in our case - e-learning material. The protection of a work is granted, whatever may be the form of its expression.

The word expression is crucial to understand the concept of copyright: Only the concrete expression of the idea is protected, not the underlying ideas or concepts. Here is an example: If you were the first person to write a spelling check programm, you would have no rights in the concept of the program, that checks spelling; you would only have rights in the actual program that you had written. However, if you copy even a few lines of a program written by someone else, this could be copyright infringement. But in this field are a lot of dark zones. Where is the border between the underlying idea and the concrete form? The more a structure of work is determined by the subject matter, the nearer you are to the underlying ideas. It is difficult to know exactly where a court will draw the line. To be protected, the original work must have a certain individuality. If it is only an assembly of information which is created just out of the structure of the subject matter, there is no individuality and no copyright protection. If you have a list of participants in an e-learning course, the layout could be a standard MS word table. There is no individuality, so the list is not protected by copyright.

A work is protected in each member country according to national rules and according to the provisions of the Berne Convention Art. 5 (1). If countries have a different level of protection, it can happen that a work is protected in one country but not protected in another country. The reasons for this situation are different levels of originality to get protection. To avoid this, the Berne Convention contains the Country of Origin Rule, Art. 5 (4) as one of the most important attempts to secure at least a minimum level of protection. With this background, a work is protected, even if the work is published in a non-member state, if the author is a national of a member state.

There are two kinds of rights which are granted to the right-owners: Moral Rights and Economic Rights. Moral Rights are indefensible, they can not be transferred. They are connected to the author's personality. The main moral rights are the Claim of Authorship and the Objection to Modifications. These rights are applicable, if two conditions are met: A use of a work must have the character of a mutilation or a derogatory action, or the use infringes the authors honour or reputation. The Economic Rights grant the economic exploitation of a work. In contrast to the Moral Rights they are transferable, they can be bought or sold like objects and ownership can change. For example, the ownership of the object changes with the fulfillment of a purchase contract. In the beginning, the seller is the owner, in the end, the buyer becomes the owner. The same can be done with Economic Rights in copyright. Economic Rights are: Translation (Art. 8) Berne Convention, Reproduction (Art. 9) Berne Convention and Adaption or Arrangement (Art. 12) Berne Convention.

There is a special connection between Moral Rights and Economic Rights: In many countries in Europe the Moral Rights remain with the author, even after the transfer of Economic Rights. So owners of Moral Rights and Economic Rights can be different persons.

As a matter of principle, the author(s) of the work are protected (Art. 1 (6) Berne Convention). The basic rule is: authors are the first owners of copyright. The author must be a national of a member state (Art. 3 (1 a) Berne Convention), but in some cases even nationals of non-member states are protected. If they have published their work for the first time in a member state, or if they are publishing simultaneously in a member state and a non-member state they are protected. A work can be published in a legal way only with the consent of

the author. If a work is published without the consent of the author, it is an infringement of the author´s copyright.

The author or owner of the right decides how a work may be used, this is guaranteed by Art. 27 (2) Declaration of Human Rights. This is a concentration of rights in a person or an institution. Such a concentration could be the death of free information flow, which we need in science. Every use would need the consent of a rightowner. Fortunately there are exceptions and privileged fields where no consent is necessary. In these fields protected works can be used without the consent of an owner of the rights. One of these fields is scientific research. We will find these provisions in the national law systems later on. The next main aspects that we have to consider, are connections between copyright and internet. In general, we can say that the rules apply in the same way to the internet. One feature of Internet seems to strengthen the idea of a world without rules: free access. Many websites have no access restrictions. The conclusion we could draw from this is: Free access means free use. But that is not necessarily so. You can compare this situation with bookshops in Germany where shelves of books are put out on display on the sidewalks. Every by-passer could get the impression that they can take a book home without paying for it. But that does not mean that each by-passer is entitled to do so. Of course they have to pay first. The same rules apply for the internet: free access does not automatically mean free use.

How can you know, whether a website component is protected or not? The well known copyright-sign © can help us. But the use of this symbol does not automatically create protection. The symbol means, a work is registered as a copyrighted work. Registration is granted only to such works, which have sufficient individuality and can be considered as an original work. In a court procedure there will be no conflict about this question and a quick decision can be achieved. A quick decision can be crucial in cases of intense ongoing infringement. But this is US law. In Germany and Italy there are no formalized registration procedures. Nevertheless, a © sign can be useful as a hint also in systems without registration procedure.

1.2 European Community

The law system of the European Community sets the framework for the law systems in Italy and Germany, so there is the need to have a look at this basic system. The European Community is based on several multilateral contracts, the first was closed in 1952. Today, 25 countries are member states; with their accession they gave up a part of their souvereignity and declared their consent to impliment the legal settings of the European Community into their national law systems [Han01] The central provisions for European Copyright are in the Directive of the Europen Community, Nr. 29 of the year 2001. Its title is Directive on the Harmonisation of certain Aspects of Copyright and Related Rights in the Information Society. The aim of this directive is the promotion of learning and culture by protecting works. In the recitals of the directive its aims are exemplified. For our purpose the following aim is important: The online service is a matter of authorisation (Nr.29). There is no total freedom. In our e-learning scenario this seems to erect borders. But there is an exception (exception means that protected works may be used without consent). This ex-

ception covers educational and scientific research purposes. There is a second exception we have to consider, because online material is a part of our subject matter. The exception includes issues of distance learning (Nr. 42). Now we are prepared to have a closer look at the directive. The directive obliges the member states of the Eurpoean Community to grant to their nationals an exclusive right to authorise or to prohibit the reproduction of their works in any form (copies in electronic form, on paper, temporary or permanent) by Art. 2. Also copying by communication to the public (by wire or wireless) is a right granted by the directive (Art. 3). This making available right is tailored to cover online access. Typical for online presentation is that members of the public get an access to works from a place and at a time chosen by them. Here are differences to the traditional right of communication to the public: The traditional right covers concrete events like broadcasting sessions or publication of books. The new making available right is not bound to a certain event any more. The next exclusive right is the distribution of a work (Art. 4). This right covers sale, rent or licensing of a work. The owners of these rights authors, performers (to this group also belong lecturers in respect to recordings of their lectures: They shall be entitled to control the exploitation of the recording), producers and broadcasting organisations; publishers also can be the owners of the rights. Some subject matters are out of scope. They are not covered by the copyright directive. These subject matters are computer programmes (Art. 1) - they are covered by the seperate directive 91/250/EEC- and data bases (Art. 1), which are also covered by the seperate directive 96/9/EC. We will discuss these directives later. Now we focus on the copyright directive which obliges the member states of the European Union to protect teaching material like text, tables, pictures, sketches and slides. As we already discussed, the concrete expression is protected, underlying ideas and principles are not protected. If we consider the situation so far, we see that there are exclusive rights which give a high amount of control to the rightholders. This control could severly block free information flow, which would be dangerous for research work. To prevent this danger, the directive provides exeptions to the excluse rights. The member states may provide exeptions (Art. 5), but they are not obliged to do it. An exception to the Reproduction Right, Art. 5, 2. (c) can be established for educational institutions and for educational purposes but not for commercial advantage, neither direct, nor indirect. Direct commercial advantage means to have commercial advantage out of the sale of the teaching material. Indirect commercial advantage is given, if a further-education department of a company does not sale their teaching material to employees, but uses it to qualify the employees. The qualifying takes place to increase the company's profit. Therefore no exception is granted.

Here we see a main principle in copyright: If someone gets commercial advantage out of a work, the rightowner shall share the profit. So commerial profit blocks the exception of use without consent. We should pay special attention to industry-founded projects. The applicability of the exception depends on the nature of the results. If the results can be used freely in research and teaching then they are within the exeptions scope. If the results belong to the industry, they are bought like a commodity. They are not open to teaching and research, there is no room for an exception. Exceptions to the rights of reproduction, communication to the public, making available, Art. 5, 3. (a) are granted in teaching or scientific research, if copyrighted works are used as illustrations for scientific discussions. If there is also a source indication with the name of the author or rightowner the use is justified by the

exception. An additional interesting topic is the Digital Rights Management (DRM). The copyright directive provides also information about the handling of digital rights management systems.These provisions also have the structure of a rule with exceptions. The rule (Art. 6, Nr. 1) says, that the member states shall provide legal protection for technological measures, which prevent copying (e.g. copy protecion on a music CD). The target of copyright protection has changed here: Not the works are subject matter of the protection, now technological measures themselves are protected. Technology to cirumvent these protecting measures may not be used. Therefore any action connected to circumvention technology is forbidden: neither the import, nor the distribution is allowed, it is not allowed to sell or rent copies or to make advertisements. This protection of digital rights management systems could be again a block against free information flow in science. But there is again an exception (Art. 6, Nr. 4): Member states shall take appropriate measures to make the work available for the beneficiary of an exception. So scientists get the right to access protected material and the rightholder gets an obligation to grant access.

Databases are protected by the Directive 96/9/EC on Legal Protection of Databases. The scope is the protection of databases in a twofold way: As the author´s own intellectual creation by copyright protection and as an object of finacial investment by the Sui Generis Right protection. Sui Generis means 'right out of itself' and is independant from the traditional requirements of copyright. It has an own commercial character. Any financial investment in obtaining, verifying and presenting content is protected. Subject matter of data base protection is the organisation of content; the form in which it is presented, not protected is the content itself. Author of a database (Art. 4) is the person who created it, in most cases, there is a legal person as rightholder but national law describes cases, in which a legal person (company, university, research institute) can be rightholder as well. The rightholder has several exclusive rights out of copyright (Art. 5). These are: the display to the public, reproduction in any form - permanent or temporary - in whole or in part, alterations, translations and distributions of copies in any form. All which may be done, only with concent of the rightholder. But there is a limitation of these exclusive rights (Art. 6, 2 b) for teaching and scientific research, if the source is indicated and if there is no conflict with normal exploitation. There is a similar structure for rights connected to the Sui Generis Right. The owner of the right (PR Nr. 41) is the producer of the database, this could be a natural or legal person who takes the risk of investment. A special right (Art. 7/ PR Nr. 41) prevents unauthorised extraction and re-utilisation of the database. Exceptions (Art. 9) are made for the use for teaching and scientific research, if the source is indicated and there is no conflict with normal exploitation. The most important result for this project, is that there are exceptions for teaching and scientific research, which allow access within reasonable limits.

The next focus is on provisions for Computer Programmes and the Council Directive 91/250/EC on the Legal Protection of Computer Programmes. Art. 1 sets the same copyright protection as for literary works. Computer programs are protected as author´s own intellectual creation and again, there is no protection for underlying ideas. If a group of authors has developed the program, the exclusive rights are owned jointly (Art. 2, 2). What is covered by these exclusive rights? First, the permanent or temporary reproduction - that covers loading, displaying, running, transmission and storage -, the translation, adaption,

arrangement - that covers any other alteration -, distribution and rental - that covers the original or any copy of the program. This utmost wide range of exclusive rights is a reaction in the fact, that computer programs can be copied so easily. In the first step an utmost amount of control is granted to the rightholders. On the other hand, the simple use of a program can be blocked by these provisions. Therefore exeptions exist also here. No authorization is necessary if a lawful acquirer (Art. 5, 1) in accordance with intended use makes a backup copy (Art. 5, 2). It is also possible to determine underlying principles and ideas of a program without consent of the rightholder (Art. 5, 3). Even a decompilation can be legally covered, if it is done for the purposes of obtaining information which are necessary to achieve interoperability with an indepently created computer program. The decompilation must be performed by the licensee or an authorised person. The results may not be used for other goals and may not be disseminated. Also the development of a competing product is forbidden.

1.3 National Law Systems Germany, Italy, India

The first countries to look at are Germany and Italy because the law systems of these countries are governed by the European Community provisions. Afterwards specific rules in India can be understood better. German Copyright Act (Urheberrechtsgesetz - UrhG) was passed in 2003. The European Copyright Directive had to be implemented in German law. Works with a certain individuality which are different from other works in the same field are protected (Sec.1UrhG). The making available right is set in Sec. 19a UrhG. There are special provision for works on internet servers: already the act of making available works by storing them on an internet server is a right which belongs to the author or rightowner. It doesn´t matter wether a work is percieved by someone else. The duration of copyright is set in Sec. 64 UrhG, it lasts for the authours lifetime plus 70 years after his death. There are exceptions for science and research in Sec. 52 a I Nr. 1 UrhG, which fall upon university lectures. It is allowed to make published works (part of long work or a complete short work) available for participants in a lecture or to use it for research (Sec. 52 a I Nr. 2 UrhG). But if an author does not wish to publish a work, this wish must be respected. Sec. 52 a IV UrhG anchors remuneration for the author, which are collected by collecting societies. Universitites negotiate periodically with collecting societies the remuneration in lump sums, to negotiate a concrete sum in every case would be too complicated.The way how to make quotations is set in Sec. 51 Nr. 1 UhrG, it is mandatory to obey quotation rules. There are also provisions for Digital Rights Management devices. The subject matter of protection is not the expression of an idea in a work (Sec. 95 a (1) UrhG) but the protection devices themselves like a copy blocker. Sec. 95 a (3) UrhG is ruling in connection to circumvention devices, that the use, advertising, import or sale of technical protected works under the UrhG is forbidden.

Exceptions for science and research are made in Sec. 95 b UrhG, but there are limits, which have to be respected. Even for science there is no right to hack, the user has the obligation to request the rightowner for an opening of the protection measures. Computer programs receive a special treatment in copyright, they are specially protected in Sec. 69

a UrhG because they can easily be copied and have a distributed technical nature. There is a peculiar exposure to illegal copying and illegal distribution. There is a wide range of rights for the rightowners, which are described in detail in the exclusive rights for authors and rightowners. In short they cover the reproduction, transient or durable ones in which form and for which purpose whatsoever. On the other hand there are explicit rights for lawful users to clear the border between legal and illegal activities. The connection between rightowners and users are mainly ruled by contracts. But there are also rights granted to the user by law, a rightowner can not revoke them, i.e. the making of a back-up copy and the study of basic ideas and principles. This belongs to the basic rule in copyright that the concrete expression is protected, but the underlying idea not, according to the agreement with the rightowner. Decompilation is allowed, if it is necessary to reach interoperability with other programms. Also in Germany a database is protected in two different ways. Copyright protected databases must be original works. The rightowner controls the use of the database and use is only permitted with the consent of the owner. The second way is, the way of investment protection. Here, the originality of the work does not matter, only the considerable effort for the creation of the work matters (like working time, money). But here are exceptions for science too. Within the limits of necessity, without commercial purpose, for own research, for lessons in universities and research institutes and if normal exploitation is not affected, the use of dababases is permitted.

Because of the European Community background, a lot of rules - even the structures of the law - in Italy are rather simular to the german law. The European Copyright Directive was implemented in Italy into the law about protection of author rights and other rights in connection, which was executed in 2004. The protected works are i.a. literary works, texts, computer programs, pictures, grafics, animations etc. (Art. 2). The right to make a protected work available to the public (Art. 16) covers the storage of a work on an internet server. The duration of protection is defined by the lifetime of the author plus 70 years, which is the same duration like in Germany. Also in Italy, there are exceptions for the use of a copyrighted work. For purposes of science and research Art. 70 (1) permits to use parts of a work in scientific discussions within justified limits as far as the regular exploitation is not affected and there is no commercial purpose behind. As an example of the affection of regular exploitation, the LAN on a university campus can be taken. One textbook can be bought, scanned and used exclusively on wireless LAN, but if this is done systematically by a central body of the university, this would be an affection of regular exploitation. Art. 70 (3) states that the information must be in quotations.

In Italy the rules for technical protection measures for digital rights management (DRM) may be used by rightowners, Art. 102/4. Access rights for science and research are settled in Art. 71/5 (2). A written application must be negociated with the Permanent Copyright Consulting Committee. There are disputes from the whole nation about this committee, because of bureaucratic delays. There are no users representatives in the committee because a conflict of interest may arise. There are permanent discussions about the role of the committee.

Art. 71/5 (2) settles a reimbursement for the rightholders. Technical protection measures may be used by rightowners (Art. 102/4), scientists can get access under certain conditions.

The conditions for access for science and research are a bit harder in Italy than in Germany.

For computer programs, there are the same considerations as in Germany: The technical nature of computer programs - special dangers by copying and distribution - ask for a wide range of control of reproduction, transient or durable in which form, for which purpose whatsoever. On the other hand, there are the usage rights. They are fixed mainly by an agreement between rightowner and user. A written contract helps to avoid misunderstandings. Some rights have to be granted to the user in every case, like the back-up copy and the study of basic ideas and principles. This is limited by the rule, that only the using of the program in a way according to the agreement with the rightowner is permitted. Decompilation to reach an interoperability with other programs is allowed, but results of the decompilation can not be use for other purposes or transfered to others, and it is not allowed to develop compeditive products. Also in Italy there are two ways of data base protection: the copyright protection in Art. 1 (protection as an original work) and the investment protection in Art. 102/2 (where originality does not matter, only the amount of work and time for the creation of the database must be considerable). A wide range of control is set in Art. 64/5. Because of the technical nature of data base the situation is similar to the protection of computer programs. The exceptions for science (Art. 64/6, para 1a) are mainly the same as in Germany.

In India, the Copyright Act was passed in 1957 and amended by act No. 49 of 1999 [T. 02]. With regard to protected works, there is no difference to the provisions in Italy and Germany (Sec. 13). The rightowner controls the publication, be it by issuance of copies (books) or by communicating a work to the public (internet server) (Sec.3). The duration of protection is shorter than the 70 years in Europe; it lasts only 60 years after the death of the author (Sec. 22). There are also provisions for science and research, which are settled in Sec. 52 (1) (a) (i). Copyrighted works may be used without consent of the rightowner, but in the interest of fair dealing, the limits of use we already know from the European Community are applicable also here: Copyrighted works may be used only within justified limits; without the affection of regular exploitation and without any commercial purpose. But this exception does not cover computer programs. In India, special dangers arise out of the technical nature of computer programs. India is a multilingual country where translations get a special importance. Therefore, there are special provisions for computer programs in Sec. 32 (1A) (4) (ii) (2). There are no exeptions for science and research, Sec. Sec. 52 (1) (a) (i). Usage rights which are independant of a consent exist in a structure similar to Europe: Back-up copies may be created, Sec. 52 (1) (a) (aa) (ii), the study of underlying ideas and principles is granted in Sec. 52 (1) (a) (ac) and decompilation for limited purposes is allowed in Sec. 52 (1) (a) (ab). It is also set as a rule, that the export of computer programs, without consent of the rightowner is prohibited. But there is an exception for exports with a science and research background. For scientists outside of India, who use one of the Indian languages, computer programs may be exported. The provision Sec. 52 (1) (p) is applicable for reproductions of unpublished works. Reproduction is allowed in institutions to which the public has access, if the purpose is research and it happens 60 years after the author's death. This long period has been set up to respect the author's wish not to publish the work. Regarding to the DRM, there are currently no legal provisions in India. Provisions corresponding with the rules in Europe are planned. In India, databases are protected, if they

have the quality of an orignal work with enough individuality. If a data base does not reach a certain level of individuality, it is not protected by copyright. There is no investment-bound database protection besides copyright protection like the Sui Generis Right in Europe, so the threshold for data base protection is higher in India than in Europe.

2 Data Protection

2.1 General Provisions

Data protection law has to balance interests which are mutually exclusive. On the one hand, there are the interests of scientists who need access to information, this is crucial for their work. On the other hand, individuals want to controll their personal information to protect themselves. Consequently, both position can not be judged as completely wrong, there is no optimum which suits both sides perfectly. So a compromise which realizes as much of both positions as possible has to be found [Pet04]. Only personal data is protected by data protection law. Personal data is information related to a natural person, like data about health (psychic deseases), economic (income, real estade details), culture (membership in a certain ethnic group) and social dates (membership in trade unions). Data is personal data, if it identifies an individual. That can happen directly or indirectly. If several parts of information form a chain which leads to the idenficiation of a person, the parts of the chain can be personal data. A certain information can be non-personal data, if it is isolated and does not lead to an indiviual. If it becomes part of an idenfifcation chain, the information changes its nature and can become personal data.

To non-personal data data protection rules are not applicable, they are not in the scope of data protection and can be used in greater freedom. One kind of non-personal data are anonymize data. Data are anonymized, if there is no connection between an information and an individual person, e.g if no name, address or telephone number is mentioned. In this case the reader of a publication would not know which indivduals were involved in a data collecting process. Direct or indirect identification would be impossible. There are two levels of anonymization: utterly anonymization and factual anonymization. In the first case, identification of individuals is not possible, in the second case, identification would be possible, but it would be extremly complex or disproportionally time-consuming. In consequence, data protection law is not applicable in both cases.

But even if the result of the anonymization process is out of the scope of data protection, the process itself is within the scope. So there is a need to look on the anonymization process. Data protection rules are applicable as far as personal data are processed. If they are separated from processing, data protection rules are no more applicable. The next general rule tells us that personal data which are not longer needed must be extinguished completely as early as possible. One of the main problems of data protection is the file-keeping for the verification of research results. Here, the private interest of extinguishing data affects the scientific interest of conservation. To find a well-balanced solution, a consideration of values has to be conducted. Such a consideration of values is a typical approach to solve

legal problems: To sort out a conflict of mutual diverging interests, the private and scientific interests must be weight against each other. The first step consists in finding arguments for both parties. Aspects weighing for private interest are a high exactitude of collected personal data, a small number of steps to identify the individual and a large scale of collected data. Apects weighing in favour for scientific interest are a necessity of personal data for research result. A high intensity of public interest and a code of conduct in the scientific community that research results must be checkable. In a second step the arguments must be balanced: Which arguments are stronger? If personal data should be kept for verification it will depend on the circumstances of the special case, even for the Culture Tech Project no general statement is possible. Each single processing of personal data was scrutinised. The result was a specific consent form, which is used within the project. Another way to bypass the data protection rules is the pseudonymization of personal data. Personal data are displaced by other data after a rule of displacement. A name could be displaced by a number code or by fantasy names like Donald Duck or Peter Pan. The connection of pseudonymized data to individual person is cognisable by applying the rule of displacement.

2.2 European Community

The European Conmmunity sets a legal framework for Italy and Germany. It is fixed in the Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. A wide range is defined. What we do within the Culture Tech Project is within the scope of the directive. So the directive must be checked closer. Art. 7 tells us in which cases processing of personal data is in compliance with the law: Unambiguous consent, contract, legal obligation, vital interest, task in public interest, and other legitimate intererests. This list does not contain what applies to this project. We are looking for a privilege for science which allows us to process data without any restriction.

The most rigid provision of the directive concerns the processing of sensitive data. Art. 8 says that the member states shall prohibit processing in the cases of racial and ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership and information about health and sexuality. For this project, health and sexuality could be a barrier, because facial and speech recognition is concerned. The directive demands a set of information to be given to the individual, this can be found in Art. 10. The individual must be informed about the purpose of processing, the recipients of his data and about details of access to his data. A controler of personal data can be sued to provide information to the individual.

Art. 11 concerns information that is not obtained from the individual. The consequences are similar, it does not matter whether personal data was obtained from the individual or from another source, e.g. database of a health insurance company. The individual has the right to object under certain circumstances at anytime. This right to object is only given on compelling legitimate grounds, e.g.: data is not correct or the processing of data is not any more legitimate. The data individual must be informed about this right and about the restrictions of the right.

The member states are authorized by the Data Protection Directive - when justified by grounds of important public interest - to derogate from the prohibition of processing sensitive categories of data where important reasons of public interest so justify in areas such as scientific research - recital Nr. 33. This sentence contains important information for the considerations of values applied to this problem. Scientific research is an important reason of public interest, which can justify an exeption from the prohibition of processing personal data. The Preliminary Consideration Nr. 39 gives us an additional assistance: It is not necessary to impose this obligation if the provision of information proves impossible or involves disproportionate efforts, which could be the case where processing is for scientific purposes. Now, the way out of the trap has to be checked closer. The most dangerous kind of data is sensitive data and as we already know, sensitive data is involved in our project. In the directive are set expemtions even for this data, there are some cases in which the processing of this data is permitted. There is no help in Art. 8 (2) which permitts processing in the cases of explicit consent by individual, employment law, vital interests of the individual and legitimate activities, but there is an additional hole in the protection for sensitive data in Art. 8 (2) in form of a blanket clause. This blanket clause permits the member states to lay down additional exceptions for reasons of important public interest to those laid down in Art. 8 (2) either by national law or by decision of the supervisory authority. If this can help us, it has to be checked later on during the examination of national law. The directive itself states not more than that. The reasons of important public interest will be a topic in national law. Art. 11 (2) covers personal data, which are not sensitive data. An exemption restricts the right of the data individual to be informed about the data processing. According to Art. 11 (2) no information to the individual is required in the case when scientific research is concerned and the provision of information proves impossible or the information of the indivudual involves a disproportionate effort or the recording or disclosure is laid down by law and appropriate safeguards are implemented to ensure the enforcement of the provisions. Member states must ensure that the information-right of the individual is restricted only in the cases written in the provision and not also in other cases. That means, the provions in the national law systems may not create any doubt about the scope of the exemptions. We will see how that works, if we come to provisions in national law. The next exemption concerns the individuals right to access his/her personal data. The access right can be restricted, if - following Art. 13 (2) - the processing takes place solely for the purposes of scientific research and the data is not used for taking measures or decisions regarding any particular individual, for example social insurance contributions may not be increased, because the participation is in a medical research project and shows a higher risk of a certain desease in the future. But an exemption of consent is not given in this provision.

2.3 Germany

The structure of the German national law system has to be explained closer. Germany is a Federal Republic, which is a compound of 16 federal states. Two of these federal states are Sachsen Anhalt (Magdeburg) and Hessen (Darmstadt). The legal framework is set at federal level, the details at state level. The legal framework is the Bundesdatenschutzgesetz (BDSG), this is the data protection law at federal level. Details are set in the Landesdaten-

schutzgesetz, this is the data protection law at state level. In German national law we find again the system of rule and exeption. The general rule is: Processing of personal data is forbidden. The exeption is: In specific cases processing is legitimate [Her05].

§ 4 Bundesdatenschutzgesetz (BDSG) provides us with the rule, that creation, processing and exploration of personal data is only allowed if this law or another statutory instrument permits it. That is not what we need for our project. The exeption which could help is laid down in § 40 BDSG concerning the processing of personal data by research institutes. Creation and internal use of personal data is legitimate if the purpose is scientific research. Personal data must be anonymized and pseudonymised as early as possible. These provisions are similar to the European Community Data Protection Directive. The publication of personal data is only legitimate, if there is a written consent of the individual. The legislation in Germany can not go beyond the European Community framework, so there is no exemption in case of publication. The reason is that publication is the most intensive danger for privacy, so the requirements are high [PR05]. These are the facts. In legal theory there are arguments in favour of our wish: The law provides an exemption of consent for scientific publications about events of historical impact. This excemption is granted because it would be impossible to do research on historical events without using personal data of the protagonists. It is wrong to convey an exemption only to this research area, because there are other research areas, which have the same nature like medical research or research concerning biometric data. But this is only legal theory. There is no judgement of a court in Germany which grants such an additional exemption. So we have to consider the consent a bit closer. The Bundesdatenschutzgesetz tells us more about the consent. The consent must be unsolicited and unambigouous, the rule is again, that there must be a written consent of the individual (§ 4a I BDSG). But there is an exeption: The consent must not be written, if it is for the intention of research and this purpose is gravely affected by the requirement of written permission (§ 4a II BDSG). In our project we would not need a consent if our work would be gravely affected by obtaining a consent. This would be the case if objective time constraints in our work would make it impossible to get a consent in time. In our project we evaluate personal data of people in interviews. This situation allows us to get the consent before an interview starts. So the exeption is not applicable in our project. The personal data created in the project do not affect important secrets of the involved states. So this additional way to the exception is also blocked. We must get the consent otherwise the individual could block the use of his or her data. § 27 Data Protection Law Sachsen-Anhalt says that the processing of personal data is legitimate if the purpose is for scientific research. Anonymisation and seperation has to take place as early and far as possible. The transfer is allowed among research for scientific purposes and also publication is legitimate if there is a consent or an event of actual historical impact is the research topic. But transfer does not cover publication [Jür]. There are special rules for publication we already know. The Federal State Law of Sachsen Anhalt may not grant more freedom than the Federal Law. There are different solutions in other German Federal States, but we can not use these solutions because the rules are only applicable in the involved federal states.

2.4 Italy

The Italian Personal Data Protection Code (passed by June 30. 2003) contains interesting provisions. Sec. 100 affects Data Concerning Studies and Researches. This Provision sets a rule for Universities and Research Institutions. They may create and process personal data by autonomous decision. Personal data may be communicated and disseminated to Graduates, Post-Graduates, Technicians, Engineers, Researchers, Professors, Experts, Scholars without consent of the individual.

This freedom is granted for the use of experts and scholars for personal data. But there is also sensitive data, which is excluded from this freedom. So we have to look further for regualtions concerning sensitive data. Sensitive data is also defined in the Italian Personal Data Protection Code. Sec. 4)1.d) defines race, ethnic origin, faith, political opinions, membership of parties, trade unions, etc. and information about bealth and sexuality as sensitive data. Processing these data is allowed under some restrictive circumstances. They are applicable for public bodies like universities. In cases expressly authorised by law they may process defined categories of sensitive data in defined categories of operation. There must also be a substancial public interest. High requirements have to be fulfilled. A first hint can be found in Sec. 98 (1.c), which permits the processing of sensiteve data for scientific puposes, if they are considered to be in substancial public interest. The first requirement (scientific purpose) is already fulfilled in our project, but there are other requirements still open. We need a law, which authorizes processing of sensitive data. One possibility is Sec. 20 (2): The law specifies scientific research as a substancial public interest. So the second requirement is fulfilled for our project. But the law does not specify categories of data and operations. Categories of data and operations meet this requirement, if they are published by a university in form of a code of conduct. This code of conduct must be approved by the Italian Data Protection Authority. The Italian project partner did not negotiate such a code of conduct. So we need a consent in Italy for processing sensitive data.

But this consent is not the only requirement. Sec. 26 (1) Italian Personal Data Protection Code requires the Garante´s prior authorisation (Garante is the short name for the Italian Data Protection Authority). So the requirements are hard: we need both - consent and authorisation. The result is more restrictive than in Germany. As usual, we look for further exeptions. We have to consider Sec. 26 (3) Italian Personal Data Protection Code. There is a list of exemptions - e.g. the processing is necessary to protect a third party´s life or the processing is necessary to comply with obligations laid down by law in the employment context. But the listed exemptions do not apply for Science/Research [Rob06].

2.5 India

Now we come to regulations in India. Currently (Spring 2006), there is no data protection law in India, but there is an ongoing legislation process [Pro06]. A draft version is currently discussed in the Ministry of Communications and Information Technology. Although India

did not sign the TRIPSs (Trade Related Intellectual Property Rights) Agreement, planned regulations are designed to be in line with European and US Legislation. One of the reasons for this orientation is the so called "Save Harbour Principle". Any transfer of personal data of EU / USA nationals to third countries is only allowed if the target country meets the EU / USA standards. The background of this legislative develpoment is the fact that European and US companies still hesitate to outsource business processes to India. If the Indian data protection law becomes effective, employees in EU and USA will be globalisation losers and employees in India are globalisation winners. India has a better position in the global low wages competition.

There are other applicable provisions. We find them in the IT Act of 2000. Sec. 72 concerns confidentiality and privacy. It protects electronic records, books, registers, correspondence, information, documents or other material and disclosure. Prior consent is necessary. This section also contains severe punishment rules: Imprisonment up to two years, fine up to Rs. 100.000 - approx. 1.770 Euros - or both.

Now we are at the end of our general view to Data Protection Basics in India, Italy and Germany. The following conclusions can be drawn: We are not as free as we would like to be concerning the processing of Personal/Sensitive Data. The processing of personal data is possible in many cases; the use of sensitive data is bound to prior consent in every case. In the internal field we have more freedom than in the public area. Publication of personal data without consent may not be based on purposes of science and teaching. We need a consent for publication. All that leads us towards a pragmatic approach: Personal and sensitive data should be used as little as possible and in an anonymised form.

3 Probative Force of Electronic Documents

The focus of this part is the role an electronic document can play in an international legal procedure.

3.1 General Provisions

We start with a survey of the functions of evidence. Evidence is every type of statement which helps to prove a fact in trial. Judges or juries have to be convinced. This can be done by oral testimony, objects, pictures or documents. Some types of information are excluded from court procedures, they are non-admissible. Unreliable information like hearsay evidence or an experts opinion based on unaccepted facts are non-admissable. There are other reasons which transform reliable information into non-admissible information. If it is too complex or too costly to present a testimony compared to its value, the testimony becomes non-admissable. This could be for example a witness of an accident who lives far away and did not see the critical phase of the accident. Non-admissible are facts that are gathered by illegal methods, like torture. This 'Fruit of the Forbidden Tree' doctrine is one of the pillars of a constitutional state.

If we consider admissible evidence, we find that there are several kinds of admissible evidence. The circumstancial evidence creates belief by showing surrounding cirumstances which logically lead to a conclusion of fact. The direct evidence creates belief by the presentation of a fact itself. Here we see that the central idea of all kinds of evidence is to create belief and trust. Court procedure takes place after the event which is subject to trial; judges did not see the event themselves. All they have is what they get in the case files and during the trial by presentation of evidence. The result of a court procedure depends not primarily on what has happened, it depends primarily on what can be proved. Therefore trust is a central aspect of evidence. A classical method to create trust is the paper document evidence. It has a traditional form, where content is written or drawn on paper. The content can be fixed thoughts, ideas, obligations, entitlements, etc., which are signed by the responsible person to clarify who is obliged or entitled by a document. Paper documents have two traditional functions: The first function is the fixation of thoughts, ideas, obligations, entitlements, which are expressed in the document. The second function is warning. The person who signs shall become aware of the obligation which comes into existance by signature. The signed paper serves as an identification of the person who is responsible for the fixed content.

How can these principles be assigned to electronic documents? We know that the central aspect of evidence is trust [AZ05]. It is also known that trust is created by two main aspects: integrity (content was not changed) and authenticity (signature by responsible person). Electronic documents must compensate two main disadvantages: There is no original tangible object for a fixation and there is no physical act of signature. The technical measurement for compensation is the electronic signature. Not all kinds of electronic signature are acceptable as a full compensation of a signed paper document.

3.2 European Community

To create an adequate amount of trust, we need an advanced electronic signature, which must be based on a qualified cerificate. The signature must be created by a secure signature creation device.What does this mean for the legal point of view? To answer this question, some rules about legal requirements on trust creating electronic signatures must be checked. Some general requirements can be found in certain European Union directives. The most important is the "Directive 99/93/EC of The European Parliament and of The Council of December 13, 1999 on a Community Framework for Electronic Signatures". The aim of the directive picks up the idea of trust. It shall strengthen the confidence in new technologies (recital 4). This generic goal becomes more strengthen, if you read recital 21: The directive shall contribute to the general acceptance of electronic authentification method and shall ensure that electronic signatures are valid in all member states of the European Union. Electronic signatures shall be used as evidence in legal proceedings.

The scope of this directive does not cover rules about the conclusion of contracts. Rules about contracts can be found in the E-Commerce Dircetive 2000/31/EC. This directive obliges the member states to ensure that contracts by electronic means (Art. 9 / 1) can have the same binding powers as a contract traditionally fixed on paper. Electronic format

may not be an obstacle for binding power. To conclude a contract, you need nevertheless binding declarations of the contract partners. This is a basic contract rule in all European countries [Alt05].

Art. 5 I of the Electronic Signature Directive determines that an electronic signature has the same legal effect like a handwritten signature and that it is admissible as evidence. Three requirements must be fulfilled. The first one is the Advanced Electronic Signature. Art. 2 Nr. 2 rules, that it must be uniquely linked to the signatory and it must be capable of identifying the signatory. It must be created by means under the control of the signatory and must be linked to the document that subsequent change of data is detectable. The second requirement for an equation of a digital signature with a written signature is the qualified certification. Features of a qualified certification out of the legal point of view can be found in the Annex I of Electronic Signature Directive. The certificate must contain the indication as qualified certificate, the identification of certification-service-provider, the name of the signatory, specific attributes of the signatory (legal roles a signatory can have like lawyer or custodian), signature verification data corresponding to signature creation data, beginning and end of validity of certificate, the identity code of certificate, the advanced electronic signature itself, limitations to scope of certificate and the limits of financial value of transactions. The third requirement states, that the signature must be created by a secure signature creation device. Annex III of the Electronic Signature Directive determines that there must be appropriate technical and procedural means. These means it must ensure the following features: Signature creation data can occur only once, secrecy is reasonably assured, signature-creation data can not be derived, the signature is protected against forgery, signature-creation data can be protected by the legitimate signatory against others, data to be signed must not be altered, and data to be signed must be prevent from being disseminated prior to the signature process.

The words *reasonable assured* tell us that creation devices must meet the state of the art, but the state of the art is changing permanent, so the requirements for the qualified electronic signature are changing dynamically. The signature must be protected against forgery, so there is a need to use the current available technology [Mau06]

Besides the qualified electronic signature there exist other kinds of electronic signatures, which do not meet the three requirements. Art. 5 II of the Electronic Signature Directive is engaged with these kinds. The most imortant information is that such a signature is still an admissible evidence and that it keeps a certain legal of effectiveness. But the probative force is weaker because it rises higher chances for objections.

The directive defines several additional principles, which all member states have to implement. Some of them are the supervision of certification-service- providers (Art. 3 Nr. 3), the supervision of secure signature creation devices (Art. 3 Nr. 4), the liability of certification-service-providers (Art. 6) and the acknowledgement of foreign certificates (Art. 7).

What has been shown till now is that there is a set of rules which has only one goal: To create trust. There is a system of requirements and control which contains explicit requirements for Signatures, Certificates, and Certification Authorities. There are also defined procedures of control, which are exercised by defined institutions with defined powers. All that has been

set up to ensure that electronic documents have the quality of integrity (content has not been changed) and the quality of authenticity (the person which appears as signer is also in reality responsible for the document).

3.3 Germany

In Germany two laws contain the main rules of producing trust. The first one is the Civil Procedure Code (Zivilprozessordnung - ZPO), which concerns is the probative force of electronic documents, the second is the Digital Signature Act (Signaturgesetz - SignG), which settles the rules for certificates, certification authorities and the control of certification authorities. We will start with the Civil Procedure Code (Zivilprozessordnung - ZPO). The main principle is the free evaluation of evidence (Sec. 286 I ZPO). The probative force of an electronic document depends on its power as evidence. Any evidence is as strong as a judge can be convinced. We can see this function of evidence in a well known German proverb saying "On sea and in front of court you are in the hands of god". But a judge can not decide really arbitrarily, he has to establish the reasons for his decision in the judgement, and a judgement can be an attacked in front of a court of a higher instance. An incorrect judgement would be repealed, so a judge must be careful.

But as so often in law there are rules and exceptions. In German evidence law, the rule states the freedom of evidence evaluation (Sec. 286 I ZPO). The exceptions cut this freedom by setting evidence rules (Sec. 286 II ZPO). Here judges are bound to a certain evaluation, they are not free in their decision anymore. Evidence rules are a great help, if you are trying to predict the outcome of a trial. For documents an evidence rule is set in Sec. 416 ZPO. Probative force of private documents is given, if they are written or drawn on paper and are signed by hand. They have full probative force, that the statement was willingly disseminated by the signer. If a plaintiff presents a contract signed by himself and the defendant, this contract binds the judge in one way: The judge must assume that the defendant gave the contract willingly after signature. The judge is not free to assume otherwise. Now let us assume that the defendant was not quite sure whether he really wanted to be bound by the contract, he deposited the contract on his desk to think it over and an employee found the contract, wanted to do his boss a favour and faxed it to the claimant. What is now the legal situation of the defendant? The judge is bound to assume that the defendant gave the contract out of his hands willingly. Only if the defendant can formally prove, that the contract was not given away willingly, he can escape the duties fixed in the contract. This is in short the function of this evidence rule [GP02]. There is a second kind of evidence, we have to consider if we are checking the probative force of documents: the circumstancial evidence. The principles of circumstancial evidences are based on case law, not on statutory law. Case law consists of principles, which are derived out of a lot of judgements. The principle of circumstancial evidence assumes that the text of a document is correct and complete. If an opponent on trial wants to attack this circumstancial evidence he must prove concrete facts, which show that the text of the document is incorrect or incomplete. This rule is only applicable for paper documents.

Given the spreading of electronic documents, it is importand to see, how electronic documents are treated within the traditional legal framework. Sec. 371 a ZPO is the central rule for the legal treatment of electronic documents in Germany. For engineers it is of value to know this provision. Is says, that an electronic document with a qualified electronic signature has to be treated like private paper documents. This means, that the evidence rule about giving away a document is applicable. Whoever has an electronic document with an electronic signature of the opponent at hand, is in a good position as far as the question of giving away the document is at stake. Also the case law principle of circumstancial evidence, which says, that the content of a document is unchanged and complete, is applicable. There are two more functions of electronic documents in court procedures. Sec. 126a ZPO requires written form, electronic form is only admissible if it is signed by a qualified electronic signature. An electronic contract in this form concerning the purchase of land would have full evidential power. Sec. 130 a ZPO concerns procedural documents like applications, pleadings, submissions, and expertises. An electronic document is admissible, but its probative force is small. A qualified electronic siganture would increase the probative force to full evidental power.

The Digital Signature Act (Signaturgesetz - SignG) defines requirements on qualified electronic signatures and on the whole procedure of producing, usage and controlling of electronic signatures.

We find a definition of electronic signature in Sec. 2 Nr.1. Electronic signature consists of data in electronic form which are attached or logically linked to other electronic data (document) and which are used for authentication. The advanced electronic signature (Sec. 2 Nr. 2) is exculsively assigned for the owner of the signature code and enables the owner to be identified. It is produced with means under the control of the owner. If it is linked to the document, any subsequent alteration can be detected. The qualified electronic signature (Sec. 2 Nr. 3) is the safest form of electronic signature. It is based on a valid qualified certificate which is produced with a secure signature-creation device. These terms describe the core elements of a qualified electronic signature, they should be explained in detail. Relevant legal requirements to a qualified certificate are defined in Sec. 7 of the Signaturgesetz (SignG). These requirements have more a formal than a technical character: A qualified certificate must include the name or unmistakeable pseudonym of the owner of the signature, the current number of the certificate, start and end of validity, name and state of certification-service provider, limitations to certain applications, declaration as qualified certificate and attributes of the signature-code owner. It must be assigned to the signature-test code. Algorithms for use in signature-test codes must be in control of the signature code owner and certification-service provider. There are also some requirements which aim to the technical features, they are defined in connection with Secure Signature Creation Devices. Secure Signature Creation Devices (Sec. 17) demand, that forged signatures or false signed data could be identified reliably and that there is protection against the unauthorised use of the signature codes. The signature codes must be unique and secret. The storage outside the device must be impossible. The possibility of falsification of time stamps must be excluded.

The requirement of "Identifying forged signatures reliably" must be checked more in detail, because here we have to face one of the big problems in dealing with law: the interpretation

of a rule. "Reliable" describes a feeling. The feeling, that something is reliable, comes into existance, if one has the impression that everything which can be done, definitely has been done. This leads us to the next question: Is there a point within the process of designing and manufacturing an electronic product, at which we can say, that everything possible has been done? Such a point may exist theoretically, but not in reality. Therefore the legal requirement of reliability means that all has been done which is within the range of the state of the art. This is enough to fulfill the legal requirement [GPI04]. For a definite assignment of a signature to a document the Secure Signature-Application Components must show (Sec. 17) to which data (document) the signature refers, whether the signed data are unchanged, the signature-code owner, the contents of qualified certificate and attributes, and the result of subsequent check of certificate. These are a lot of requirements. All of them aim to the creation of trust. But how can someone be sure, that these requirements are really fulfilled? By establishing liablitiy of the certification-service providers (Sec. 11). The certification providers are the key players. If the key players can be forced to obey the rules, any user can trust the signatures. So the law states, that the infringement of requirements leads to a reimbursement of third parties damages which were suffered from relying on the certificate or time stamp. The liability is connected to users relying on digital signatures, here we find again the element of trust. And the law provides an additional element of reliablity, the Compulsory Cover (Sec. 12). It imposes appropriate financial penalties, the minimum of damages is set to 250,000.00 EUROS. To get permission to offer qualified signatures, the staff members must show a specialised knowledge (Sec. 4, para 2), this means, they must have sufficient knowledge, experience, and skills. The last point of this survey is about international acceptance of foreign electronic signatures and products for electronic signatures (Sec. 23). All members of the European Union have the same legal requirements concerning hand written signatures, so electronic signature is admissible as evidence in legal proceedings within the European Union. If other countries have legal requirements in the same manner concerning written signatures, they are admissible as evidence in legal proceedings, but the minimum is the advanced electronic signature. All these regulations lead to an enormous infrastructure, which has only one intention: to creat trust [AZ05]. On the other hand: The infrastructure is too big and too complicated for a lot of people. As a result, the advanced electronic signature is not popular in Germany [DMK+06].

3.4 Italy

In Italy, the applicable rules are also spread over a multitude of acts. The most important rules for us are the Italian Codice Civile (CC), where evidence rules can be found, and the decrees implementing the EC Signature Directive. A main principle of this rules is, that the probative value of the electornic signature depends on the kind of signature. Italian law knows the electronic signature as data in electronic form, which is attached to a document as a method of authentication. This is the lowest level, there are no specific requirements for signatures, devices or certificates. The features of the advanced electronic signature are the features described in the EC Signature Directive. The Digital Signature unites the advanced electronic signature with a public key infrastructure [LR04]. We will recognise the core principle of a connection between the quality of a signature and the evidential value in the

following evidence rules: An electronic document without a signature does prove facts (free evaluation) but it does not prove the connection between the document and a certain person (Art. 2712 CC). Electronic documents with electronic signatures allow free evaluation of quality and security (Sec. 116 Civil Process Code). The evidential value can be strong or weak; this depends on the circumstances and whether the originality of the document is attacked. An electronic document with advanced or digital signature has the same probative value as a private deed with a handwritten signature (Art. 2702 CC). To assure the security level of the advanced and digital signature, there are several special rules. We start with a decree from the year 2002, when the implementation of the EC Electronic Signature Directive was established. The definitions of electronic signatures, certificates, secure signature creation devices and the accrediation of certifications service providers are set in Sec. 2, all these definitions are according to EC directive and we know them by now. In this decree, further regulations on quality standards for Certification Authorities (Sec. 5), liabality of Certification Authority (Sec. 7) and compliance of secure signature creation devices with EC Directive (Sec. 10) can be found. Now we turn to another decree, to the Decree of April 7, 2003 No. 137. It is about the adaption of other rules with connection to the probative force of electronic documents. The following enumeration shows that a national law system is networked to a high degree and that an alteration of rules at one point leads to consequences in other fields: documents in public administration (Sec. 3), payments by telecommunication (Sec. 5) and replacement of seals, punches, stamps, tokens, marks (Sec. 9). All these regulations deal with the validity of electronic documents with advanced digital signatures. This decree covers also the Quality Assurence for Certification Authorities regarding the organisation, the technical equipment, the financial background and the staff. The detailed rules for accreditation are also similar to the rules in Germany. Now we turn to a decree of January 13, 2004. It gives us a set of technical rules concerning the key characteristics (Sec. 4), the generation and storage of keys (Sec. 6,7), information in certificates (Sec. 15), revocation of certificates (Sec. 17), security plans for certification authorities (Sec. 30) and a public list of certification authorities (Sec. 41). All these provisions are similar to rules in the German Digital Signature Act; both laws are compliant with the EC directive on Electronic Signatures. Now we have an idea of the system in Europe and we can turn to India.

3.5 India

Again the most important rules are spread over the legal system, due to its netlike complexion. We find rules, inter alia, in the Information Technology Act and in the Indian Evidence Act. We start with the Indian Information Technology Act, which was passed in the year 2000. It sets the rules for Authentication of Electronic Records (Sec. 3) by affixing the digital signature with a symmetric crypto system and a public key infrastructure. It regulates the Legal Recognition of Electronic Records (Sec. 4) too, which means, that the written form on paper can be substituted by electronic form. This definition of digital signature is similar to the definition of the advanced electronic signature in Europe. But that does not say anything about authenticity. Nothing is fixed, which concerns a signature as a measure to link a certain person to a certain document. This link is decribed in Sec. 5 (Legal Recogni-

tion of Digital Signatures) which says, that any electronic document with a digital signature shall be presumed to be of the originator. The legal framework for Certifying Authorities is set in the IT Act too. The requirements on qualification, expertise, manpower, finances and infrastructure can be found in Sec. 21, they are similar to the requirements in Europe. The background is the wish to participate in the international e-commerce. The controller of Certifying Authorities is appointed by the Central Government (Sec. 17), his duty is to supervise the standards of technology, organisation, staff and finances (Sec. 18). Details of the Digital Signature like identitiy of signatory, name of certifying authority, qualification of staff members, etc. are set in Sec. 35-38. We know these details from the rules in Europe.

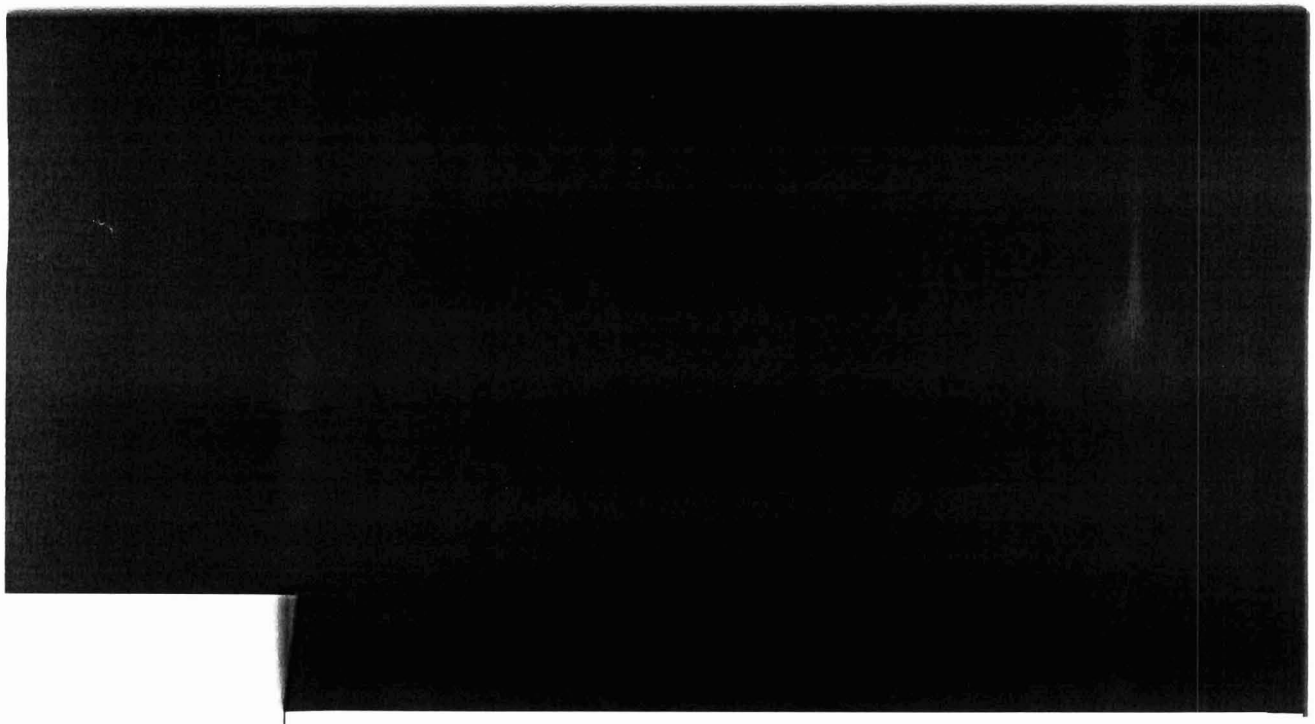
The Indian Evidence Act was amended in a lot of details. Some examples are electronic records and how they are admissible in court procedures (Sec. 65 B), the secure digital signature, where a connection between an electronic document and the subscriber must not be proved (Sec. 67 A), and the non-secure digital signature, where the court may summon a member of the certification authority or controller as witness (Sec. 73 A). The secure digital signature is defined in Sec. 15 IT Act as a unique fixation, which is capable of identifying the subscriber, who controlls the device. These regulations are similar in Europe. Now we see two examples of legally covered presumptions. In these cases a court has to take a fact as given without further scrutiny. Against the assumption that the contrary can be proved but this would be a duty of the party, not the duty of the court. These presumptions are instruments to reduce the duration and complexity of a court procedure. They are like evidence rules in Europe. For us, the following presumptions are interesting: For the secure digital signature (as defined in Sec. 15) the court assumes, that the electronic record has not been altered (Sec. 85 B) and regarding the Digital Signature Certificate the court assumes, that the information in the certificate has not been changed (Sec. 85 C).

Now you have a survey of regulations on electronic documents in court procedures. The system in India requires the same enormous infrastructure as in Europe. It remains to be seen, whether the further development in India will face the same difficulties as in Germany and Italy. As a result we can see that rules for electronic documents are harmonised to a high degree. We have a comparable legal framework in India and Europe.

4 Virtual Presence in International University Examinations

4.1 General Provisions

In this chapter a concept for replacing the traditional physical presence in university examinations by a virtual presence will be discussed. Due to the highly formal character of university exminations the virtual presence shall be secured and documentated in a way which leads to legally effective electronic documents. The main aspects that will be elucidated are the function of physical presence, the legal framework in universities, the document features oral examinations, and document features written examinations.



The physical presence in oral examinations has several functions. Of course it shall prove the identity of the candidate and the integrity of direct communication. It shall be possible for the examiners to evaluate immediate answers to questions and contributions to a discussion. Examinators shall have the possibility to test the technical and social skills of the candidate. Interaction with the candidate is the basis for evaluation. So a virtual presence in oral examinations is possible, if there is an electronic document, which provides equivalent information to a face to face encounter. The document must provide the impression of the candidate with regard to physical appearence, voice, tempo of activity, clearness, coherence of reasoning and record of the discussion as a process.

Now we should throw a glance at the functions of physical presence in written examinations. The physical presence shall ensure the identity of the candidate and his activity. He/she shall prove that he/she is able to give the defined output within a defined timeframe. The physical presence shall grant equivalent circumstances for all candidates, no one shall enjoy a more helpful environment than the others. The most critical element here is the exclusion of forbidden recources. The electronic document must prove that the candidate had no possibility to get additional information about the subject matter for the written examination. This was the discussion of the functions of physical presence in examinations and a first step to the features which an equivalent electronic document shall provide to cope with these functions.

The next element to be checked is the legal framework in universities, to find out whether an electronic document should provide additional features to comply also with the legal framework.

4.2 Germany

In Germany, there are regulations in several levels, because Germany is a federal state like the US. In the federal level is stated, that examinations have to be formally organised in examination regulations. The states are responsible for setting up the rules. In the state Sachsen Anhalt, of which Magdeburg is the capital, examination regulations are set by the universities in cooperation with the state. These are exam regulations of the Computer Sciences Department of the Magdeburg University: There are two forms of exams (Sec. 4 / 4), a written examination and an oral examination. It is set, that the examiner must be independent and there must be an evaluation of the candidates contributions. So far there are no additional features required for electronic documents. The regulations of the Computer Science Department in Magdeburg concerning written examinations also give us some hints in Sec. 9: The candidate shall prove that he is able to find solutions for problems within limited time and with limited resources. So our electronic document must record start and end of the time slot and it must record and prove that the candidate did use only admissible ressources. There are also some rules for oral exminations in Sec. 9: The candidate shall prove knowledge of the coherence of a subject matter. This should take place in front of an examiner with one or more candidates at a time. The results must be kept in minutes. Out of this rule we can draw the additonal requirement, that also actions of more than one candidate must be recorded and that a protocol must be created. The electronic protocol

must provide the same kind and amount of information which is recorded by a traditional paper protocol. There is also a rule concerning international cooperations. (Sec. 7 / 2) requires, that syllabus examination requirements and substance as well as amount of subject matters must be equivalent to German standards. The candidate has a right to read his examination files (Sec. 36) up to one year after the examination.

4.3 Italy

In Italy, a lot of leeway is given to the professors at the University of Florence. The exam regulations leave the details of the procedure to the discretion of the professor. The aim of the examination is the demonstration of knowledge of the coherence of a subject matter. The student has to keep a report book containing the subject, date, mark, signature of lecturer. The examination minutes must include the registration number of the student, the subject, date, mark, questions, arguments and the signatures of examiners. The conservation of documents is again in the discretion of the examiners. It is only stated, that the conservation should last at least up to the discussion with students.

4.4 India

Now we turn to regulations in India, especially to the Indian Institutes of Technology (IIT) Chennai and Kharagpur. The IITs have a more independant status than universities and a more independant status of professors. There are more individual decisions of course instructors concerning the acceptance of exam results and the acceptance of foreign students. First we consider the Exam Regulations in IIT Chennai. As a legal framework there are ordinances, which require (R. 16.0) lecture / tutorial based subject quiz tests, lecture based subject, end semester examination (three hours duration) and project evaluations as a project report and an oral examination. The course instructor is supreme in dealing with the evaluation, there is no fixed procedure. The custody period has a duration of approximatly 6 months, it depends on the decision of the instuctor. These details show us, that the amount of freedom for a professor in IIT Chennai is much higher than in Magdeburg/Germany. In IIT Kharagpur the exam regulations also grant a lot of freedom to professors. There are different densities of formal requirements. The most formal events are the final exams. The regulations are the following: A written examination with physical presence in examination center is required. The candidates have to answer identical questions within a fixed time. The requirements for the mid semester exam are identical, but the teacher chooses the form of attendance, assignment and decides if it is a class test or individual test. There is no duty of custody, exam results must not be kept longer than until the final discussion.

Some general conclusions can be drawn of these facts: Despite of the different density of regulation in India, Italy and Germany, some features can be found, which are common in all project universities. Document features for oral exminations shall provide equivalent information about the impression of the candidate in terms of physical appearence, oral, the tempo of activity and the clearness and coherence of reasoning. Equivalent information about the actions of the examiners and candidates must be granted also. It must be

assured, that no additional resources can be used, so there is the need of a prepared room for candidates and a confirmation of correct conditions by staff members of the involved universities. To make the documentation safe, there is a need for audio-video equipment, digital watermarks and an electronic signature of examiner. There is no need of a longterm storage, only short custody periods are required. Now the document features for written examinations have to be checked. The application features for written examination shall provide equivalent information about the impression of the candidate (audio, video), give a reliable identification of the person, the time frame and the exclusion of additional resources. There must be a prepared room for the candidates, and a confirmation of correct conditions by the staff members of the foreign university. While the exam takes place, there must be periodical video and audio checks.

A final conclusion can be drawn: It is theoretically possible to create documents, which preserve those elements for an examination, being necessary to evaluate the candidates contributions and to prove the candidate's identity. There is no law, which expressly prohibits the substitution of a physical presence by a virtual presence. But the trust-creating power of our electronic documents has to be strong to provide a sufficiant level of reliability.

5 Acknowledgement

The authors would like to thank all project partners for contributing information which made it possible to adapt the presentation of legal aspects close to the projetc partner's needs. The work described in this article has been supported by the EU-India cross cultural program. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies.

Bibliography

[Adr03] Adrian Sterling. *A World Copyright Law*. Sweet and Maxwell Publishers, 100 Avenue Road Swiss Cottage, 2003.

[Alt05] Alty van Luijt. *Beyond DRM: Balancing of Interest, in: Distribution und Schutz digitaler Medien durch Digital Rights Management, Pages 61 - 74.* Number ISBN 3-540-23844-1. Springer, Tiergartenstrasse 17, D-69121 Heidelberg, 2005.

[AZ05] Andreas U. Schmidt and Zbynek Loebl. *Legal Security for Transformations of Signed Documents: Fundamental Concepts in: Lecture Notes in Computer Science vol. 3545/2005, pp. 255-270.* Number 978-3-540-28062-0. Springer, Tiergartenstrasse 17, D-69121 Heidelberg, 14November 2005.

[DMK+06] Dragana Damjanovic, Michael Holoubek, Klaus Kassai, Hans Peter Lehofer, and Wolfgang Urbantschitsch. *Handbuch des Telekommunikationsrechts.* Number ISBN 3211838953. Springer, Tiergartenstrasse 17, D-69121 Heidelberg, 1 August 2006.

[GP02] Gerhard Lüke and Peter Wax. *Münchener Kommentar zur Zivilprozeßordnung. Aktualisierungsband ZPO-Reform.* Number 3406484174. C.H. Beck, Wilhelmstraße 9, D-80801 München, 31October 2002.

[GPI04] Gerald Spindler, Peter Schmitz, and Ivo Geis. *TDG : Teledienstegesetz, Teledienstdatenschutzgesetz, Signaturgesetz ; Kommentar.* Number ISBN 3-406-49548-6. C. H. Beck, Wilhelmstraße 9, 80801 München, 2004.

[Han01] Hans Georg Fischer. *Europarecht, 3. Auflage.* Number ISBN 3-406-48370-4. C. H. Beck, Wilhelmstraße 9, D-80801 München, November 2001.

[Her05] Hermann Christoph Kühn. *The Implementation of the Data Protection Directive 95/46/EC in Germany in: Implementation of the Data Protection Directive in Relation to Medical Research in Europe,pages 121 - 140.* Number 0754623696. Ashgate Publishing, Gower House, Croft Road, Aldershot, Hants GU11 3HR, 30January 2005.

[Jür] Jürgen Ancot. *Sächsisches Datenschutzgesetz, Kommentar.* Number ISBN 3415032000. Boorberg Verlag, Scharrstraße 2, D-70563 Stuttgart.

[LR04] Luigi Martin and Roberto Pascarelli. Electronic signature: value in law and probative effectiveness in the italian legal system. *e-Signature Law Journal, vol. one, pp. 17-23,* 31January 2004.

[Mau06] Maurice H. M. Schellekens. *Electronic Signatures: Authenticaton Technology from a Legal Perspective.* Number 9067041742 in IT and Law. Asser Press, P.O. Box 16163, 2500 BD The Hague, The Netherlands, 3 February 2006.

[Pet04] Peter Carey. *Data Protection: A Practical Guide to UK and EU Law.* Number 0199265682. Oxford University Press, Great Clarendon Street, Oxford ox2 6dp, 6 May 2004.

[PR05] Peter Gola and Rudolf Schomerus. *Bundesdatenschutzgesetz: BDSG, Kommentar 8. Aufl.* Number ISBN 3-406-49548-6. C. H. Beck, Wilhelmstraße 9, D-80801 München, 2005.

[Pro06] Probir Roy Chowdhury. Update: India - service tax, data protection and customs rules, pages61 - 62. *Computer Law Review International,* 30 April 2006.

[Rob06] Roberto Lattanzi. *Processing of Personal Data and Medical/Scientific Research within the Framework of Italy's Legal System in: Implementation of the Data Protection Directive in Relation to Medical Research in Europe, ; pages 193 - 208.* Number 0754623696. Ashgate Publishing, Gower House, Croft Road, Aldershot, Hants GU11 3HR, 30January 2006.

[T. 02] T. Ramappa. *Intellectual Property Rights Under WTO: Tasks before India.* Number 817544214X. A H Wheeler Publishing, Lal Bahandur Shastri Marg, Allahabad, Uttar Pradesh 21 1001, India, 1 January 2002.