IRIE
International Review of Information Ethics
Vol. 3 (06/2005)

Thomas Hoeren:

Law, Ethics and Electronic Commerce

Abstract:

Unlike the Internet community had expected electronic commerce does not lead to an anarchic dissolution of law. In the context of electronic trade, problems arising between users and providers can be solved, for instance by applying traditional principles of contract law. And yet, the legal dispute of Internet related facts and circumstances gives rise to a number of interesting topoi. Even though these subjects have already been considered in the past (for instance in the context of satellite technology), they only now show their specific explosive effect and diversity in the face of the electronic commerce.

Agenda

The Phenomenon of Dematerialization and the new Property Rights 47
Information 47
Domain 48
Electronic Commerce and the Deterritorialization of the Law 48
Problem Areas 48
Possible Solutions 49
The Internet and the Extemporalization of Law 50
Problem Areas 50
Possible Solutions 50
Self-regulation instead of State Regulation 51
Data Protection and Depersonalisation 51
Technology instead of Law 51
Electronic Commerce and the Problem of Trust 52
Trust in the "Analogous" Environment 52
Trust and Digital Signature 52
Summary 53

Author:

Prof. Dr. Thomas Hoeren:

- Organization and contact address: Westfälische Wilhelms-Universität Münster, Institut für Informations-, Telekommunikations- und Medienrecht, Leonardo-Campus 9, 48149 Münster, Germany
- Telephone, email and personal homepage: ☎ + 49 – 251 – 83 – 38600, ✉ hoeren@uni-muenster.de, 🖳 http://www.uni-muenster.de/Jura.itm/hoeren/mitarbeiter/hoeren.htm
- Relevant publications:
  - Nutzungsbeschränkungen in Softwareverträgen - eine Rechtsprechungsübersicht, in: RDV 2005, pp. 11-14.
  - Der 2. Korb der Urheberrechtsreform - eine Stellungnahme aus Sicht der Wissenschaft, in: ZUM 12 (2004), pp. 885-887.
  - Informationspflicht im Internet - im Lichte des neuen UWG, in: WM 2004, pp. 2461-2470.
  - Recht der Access Provider, München (C.H. Beck) 2004.
  - Urheberrecht und Verbraucherschutz, Münster (LIT) 2003.
  - Grundzüge des Internetrechts, E-Commerce, Domains, Urheberrecht München (C.H. Beck), 2. Aufl. 2002

ISSN 1614-1687

The Phenomenon of Dematerialization and the new Property Rights

The first striking topos of the Internet law is the net-inherent dematerialization, which leads to a situation where material assets lose their significance in favour of new intangible assets.[1] Traditionally, the European civil codifications such as the Code Napoleon and the German Civil Act are based upon the dichotomy of goods and services.[2] Assets which could be worthy of protection but do not show the characteristics of neither goods nor services do not gain protection under present private law. This phenomenon is rooted in the logic of the 19th century. At the threshold from farming to an industrialised society the old civil law codes had to reflect the primacy of the production of goods. Even in view of the needs of a modern service society it could only refer to rudimental legal regulations in relation to service contracts. However, in a so called information society a number of legal interests exist which do not fall within the logic of goods versus services. In that respect we are dealing with new property rights, assets worthy of protection, for which traditional instruments of the civil law cannot provide security.

Information

First of all, it is a question of information as such[3]. Traditionally, the protection of information is confined to the protection of know-how as it is firmly established in the traditional regulations on trade secrets. These provisions are puzzling in a number of ways. They secure a high level protection without sufficiently defining the term "trade secrets". However, modern efforts to re-define the legal protection of "information" are facing very much the same problem. Intellectual property law is based upon the idea of a protection of works of art, literature and music and has not been adjusted to the needs of a modern information society.[4] Although the European Commission is trying to initiate such a convergence by establishing a new property right for collections of information[5] in the European Database Directive[6], the outlines of this new system of protection have not been clearly defined. Nobody knows, for example, what is meant by a qualitative or quantitative substantial investment, a necessary qualification for the sui generis protection of databases. This symbolises the basic dilemma of information law: definite criteria for the assignment of access to information and exclusive information rights do not exist[7]. The idea of an international system of information regulation ("Wissensordnung")[8] remains a mere utopia[9].

---

[1] See *Bercovitz*, Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil 1996, 1010 (1011).

[2] Compare considerations in *Hoeren*, Gewerblicher Rechtsschutz und Urheberrecht 1997, pp. 866.

[3] Compare with *Hoeren*, Information als Gegenstand des Rechts, Addendum to Multimedia und Recht 1998, No. 6, 6*.

[4] Justified in so far the fundamental criticism by *Barlow*, The Economy of Ideas: a Framework for Rethinking Patents and Copyrights, in: WIRED 2.03, 1994, pp. 84; for reformatory propositions see *Zweiter Zwischenbericht der Enquete-Kommission Zukunft der Medien, Neue Medien und UrheberR*, 1997, and *Schricker*, UrheberR auf dem Weg zur Informationsgesellschaft, 1997.

[5] See i.e. *Bechtold*, Zeitschrift für Urheber- und Medienrecht 1997, p. 427; *Berger*, Gewerblicher Rechtsschutz und Urheberrecht 1997, p. 169; *Dreier*, Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil 1992, pp. 739; *Wiebe*, Computer und Recht 1996, pp. 198.

[6] Directive *96/9/EG of. 11.3.1996, OJ No. L 77 of. 27.3.1996, 20.* See articles by *Gaster*, Ent.LR. 1995, pp. 258, *Gaster*, ÖSGRUM 19 (1996), pp. 15; *Gaster*, Revue du Marché Unique Européen 4/1996, pp. 55.

[7] Compare with the thesis by *Druey*, Information als Gegenstand des Rechts, 1995, pp. 441.

[8] Fundamental *Spinner*, Die Wissensordnung, 1994, especially at pp. 111.

[9] In so far the innovative considerations concerning the reformation of the data protection law by *Kloepfer* are not convincing. In his expert opinion for the next DJT, *Kloepfer* demands the passing of a Federal Data Act (Bundesdatengesetz) respectively of an Information Code/Statute Book (Informationsgesetzbuch), even though the particulars of such an information order would not be identifyable.

Domain

But other new property rights exist besides the information as such. Their legal fate is unclear. One of these new rights is the domain.[10] The domain represents the virtual identity of the provider and his products. Today, in the Internet a person is mainly present via such a clearly assigned domain. The domain is the conditio sine qua non for any Internet appearance and therefore also features as part of the trade name, on visiting-cards, brochures and in advertising copies. Typically, property rights are being granted by public administration working as guarantors for distributive justice. In the case of domains however the state only takes repressive actions. This can be seen as a novelty. Following the principle of "first come first served", domains are being granted by institutions under private law. A third person can only subsequently take action against such an award, drawing attention to the fact that the assigned identification could infringe the right to his own name. The state will then prohibit any further use of the domain by the domain-holder.[11] Yet, the state refuses to change the system of marketing domains[12].

But indeed, the identifying power of a domain is diminishing. First, search engines are becoming more and more important as a means for defining the virtual identity of the provider[13]. Taking into account the tremendous speed with which the World Wide Web is growing, the question of investigation for information is a pressing one. Lost in cyberspace – the feeling of getting lost in the www whilst searching for a specific homepage can no longer be taken under control simply by referring to the existing domain of a provider. An efficient supply of information is to an increasing extent guaranteed by search engines. In the future, intelligent robots will assist the user when searching in the net; the user simply defines the topic for which he seeks information in general terms and receives this information periodically in easy to digest portions from the www-robot. This upheaval gives reason to reflect the identifying power of domains. In the end, a user will hardly make use of a domain in order to find a provider. It is more likely that he will act through search-engines and robots without the domain being of any importance.

Electronic Commerce and the Deterritorialization of the Law

In the Internet, all provisions referring to the place, the territory or the seat are losing sense. The electronic speed deterritorialises the law[14].

Problem Areas

The diminishing relevance of territory-based rules is primarily demonstrated in the area of international civil procedure law and of private international law. Due to their origin in the 19th century idea of sovereignty these provisions very often refer to local connections. This is for example the case when the defendant's domicile appears as the connecting factor. Something similar applies to connecting factors such as the place where the damaging act has been committed and the place where the damaging act takes effect when dealing with questions of the law of torts or the place of contract of con-

[10] Compare from recent literature *Bettinger*, Gewerblicher Rechtsschutz und Urheberrecht 1997, p. 402; *Omsels*, Gewerblicher Rechtsschutz und Urheberrecht 1997, p. 328; *Stratmann*, Betriebs-Berater 1997, p. 689; *Ubber*, Wettwerb in Recht und Praxis 1997, p. 497; *Völker/Weidert*, Wettewerb in Recht und Praxis 1997, p. 652; *Wilmer*, Computer und Recht 1997, pp. 562.

[11] Related questions of "identification law" (names/marks etc.) will not be reduced by the fact that a number of top-level-domains will be available in the future; this new way of conferring domains will only multiply the problem of an exact/accurate assignment of domain names. See *Bettinger*, Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 1997, 404 (at p.420); *Kur*, Computer und Recht 1997, pp. 325.

[12] So at least the *Krupp*-decision *OLG Hamm*, Multimedia und Recht 1998, 214 with comment by *Berlit*, Neue Juristische Wochenschrift-Rechtsprechungsreport 1998, 909 = Computer und Recht 1998, 241 with comment by *Bettinger*. For a different opinion see, for example, *LG München I*, Computer und Recht 1997, p. 479; *LG Frankfurt a.M.*, Multimedia und Recht 1998, 151; *LG Düsseldorf*, Computer und Recht 1998, 174.

[13] See *Wilmer*, Computer und Recht 1997, pp. 562.

[14] See *Vief*, Digitales Geld, in : Rötzer (Hrsg.), Digitaler Schein, 1991, p. 117, 130.

sumer contracts. But other areas of law are also affected by connecting factors which are determined by a locality. Reference has to be made to the tax law term of the permanent establishment[15], which creates difficult questions especially in relation to the Internet.

But also in the area of online contracts, territorial criteria are very often misleading. Above all, attention has to be drawn to contracts which provide for regional restrictions of the right of exploitation, as it is for example typically in the case for television licences or distribution agreements. Such categories of contracts lead to unforeseeable difficulties when dealing with the question of use of film material or product advertising over the Internet.

Furthermore, territoriality as a connecting factor causes problem in relation to injunctions. These claims are traditionally limited to the prohibition of a specific act in the territory of a specific state; an injunction which takes effect beyond the borders of the territory of a state would not be enforceable for reasons of public international law[16]. However, in relation to Internet infringements this would result in a situation where injunctions become unenforceable because of technical reasons. A provider cannot exclude the on-line access of a homepage by a user situated in a specific state territory. In the Internet it is impossible to define user groups on a territorial basis; no one knows whether the user of the address hoeren@aol.com is situated in Germany, the USA, or Malaysia. This forces courts to define the extension of injunctive reliefs in broader terms than legally permissible. The prohibition does not only extent to the possibility of having access to a server from Germany. It has to prohibit the whole use of a particular homepage throughout the world[17].

Possible Solutions

The question is indeed how the law should respond to its deterritorialization. The problem of territoriality might be solved by creating a virtual space. All actors in this "Cyberspace" have their own net-identity which only shows a minimal connection with the domicile or the place of business[18]. Within this space, providers have to reveal their identity as it is in fact intended by the EU Directive on Electronic Commerce.

This directive however does not solve the questions of private international law which still considers the seat, the place of business or the domicile of the person affected. Here, the principle of territoriality should be replaced by the concept of purported use. This concept has mayor roots in competition law[19] and defines the applicability of national statutes according to the place where the deliberate intervention in the market takes place. Someone who uses the Internet for advertising has to do so according to German law only to the extent to which it is intended for the German market. This rule is now also being discussed in relation to criminal law[20]. Furthermore, it shows similarities with the American "minimum contacts principle". However, the copyright lawyers have always rejected to apply this principle to intellectual property law by arguing that these rights are based upon territorial a jurisdiction could only confer copyrights and trademarks within its territory. But this gives rise to the inevitable dilemma that a provider – due to the global possibility of on-line retrieval – has to be familiar with and comply with the industrial property law of every jurisdiction[21].

---

[15] For a general overview see *Vink, Albarda and others*, in: Caught in the Web, 1998, pp. 58; *Lejeune and others*, European taxation 1998, pp.2.

[16] For a short period of time, a different view has been adopted in the Netherlands in the *De Corte Geding*-decisions; see in this context *Brinkhof*, European Intellectual Property Review 1994, 360; *Gielen/Ebbink*, European Intellectual Property Review 1994, 243.

[17] *KG*, Neue Juristische Wochenschrift 1997, p. 3321 – Concept Concept.

[18] See *Turkle*, Leben im Netz, 1998, p. 9.

[19] See the decision of the Federal Supreme Court *BGHZ* 113, 11 (15) = Neue Juristische Wochenschrift 1991, 1054 – Kauf im Ausland; similar *OLG Karlsruhe*, Gewerblicher Rechtsschutz und Urheberrecht 1985, 556 (557); *Kotthoff*, Computer und Recht 1997, pp. 676.

[20] *Hilgendorf*, Neue Juristische Wochenschrift 1997, pp. 1873.

[21] The different possibilities of solution are discussed in *Hoeren/Thum*, ÖSGRUM 20 (1997), pp. 78. See also BGH, Multimedia und Recht 1998, 35 with comments by *Schricker* – Spielbankaffaire.

The Internet and the Extemporalization of Law

But even the element of time is becoming more and more absurd in the Internet.

Problem Areas

First aspects of the increasing digital detemporalization can be found in the law of copyright. Traditionally, European legislators distinguish in copyright law between the material and immaterial exploitation of works. Immaterial exploitation refers to broadcasting and TV where an unlimited audience can see and/or listen to works simultaneously. In the Internet, services are however done successively. They are not distributed to users; the users themselves are getting access to a server at a time of their own choice. Generally, the Internet is characterized as a huge collection of services on demand. In this situation one could try to apply rules for public display by analogy to services on demand. However, this (typical German) way has lost significance in the face of the decision of the international community of states to introduce a new right of "making available to the public" into copyright[22]. This solves the problem of the categorisation of services on demand; storing information for demand already constitutes an infringement of the exploitation rights of the owners of copyright and neighbouring rights[23]. Yet, this new right will cause follow-up problems such as the distinction between public and non-public in the so called *intra*net and the integration of the new right into the system of statutory exceptions.

The phenomenon of detemporalisation also influences consumer protection law. Consumer protection can be done by giving the user time to reconsider and withdraw contractual decisions. This protection is predominantly guaranteed by the introduction of the revocation right and the compulsory requirement of a written form for contracts. To that extent, the EU Distance Selling Directive is of great importance. This directive shows the dilemma of consumer protection in the digital context. Following the directive, a right of withdrawal from electronic orders will be introduced throughout Europe (Art. 6 I 1 and II), as well as the obligation to inform the consumer in that respect (Art. 4 I lit. F). But for a number of services this right of withdrawal will be denied even though substitutes have not been developed (Art. 3 I and II). In that respect, the directive leaves a number of gaps in the protection of electronic consumers.

The problem of time is also dealt with in the discussion concerning the electronic form[24]. It is already a kind of religious belief within the European Internet law community that the digital signature might be the functional equivalent to the hand-written form. When complying with the rather high security standards, a digital signature does indeed fulfil most functions of the hand-written signature. However, at the same time the warning function of handwriting has been ignored. The process of signing something in hand-written form draws the signatory's attention to the fact that he is about to act in a legally relevant manner. This warning lapses when digital signatures are being automatically generated and sent within fractions of a second. Asymmetric encrypting techniques deconstruct the temporal context; the factor of time will only subsequently be recorded in the mailing protocol.

Possible Solutions

The digital loss of time has to be compensated; there should be a substitute for legal rules which make reference to time. For example, when substituting the written form for electronic equivalents, the user closing a contract should be granted a pause during which it is possible for him to reflect whether he actually wants to give an expression of will with such content. This might lead to a revocation right which allows the declaring party to revoke electronic orders after the expression of will has been received. The Distance Selling Directive introduces such a right of withdrawal for consumers. Facing the speed of communication in the net, this provision should be extended to all declaring parties, irrespective of their consumer characteristic, in order to allow everybody time to reflect.

---

[22] See Art.8 WIPO Copyright Treaty.

[23] See *Lewinski*, Multimedia und Recht 1998, pp. 115.

[24] Compare *Bizer/Hammer*, Datenschutz und Datensicherheit 1993, pp. 619; *Ebbing*, Computer und Recht 1996, pp.271; *Heun*, Computer und Recht 1995, p.2; *Kilian*, Datenschutz und Datensicherheit 1993, pp. 607; *Pordesch/Nissen*, Computer und Recht 1995, pp. 562.

Self-regulation instead of State Regulation

The amount of problems surrounding the enforcement of law results in a growing number of voices calling for self-control and self-regulation in the net. In the present discussion, there is strong emphasis on the so called Netiquette and other methods of voluntary self-regulation by providers. However, only little attention has been to the fact that "the" netiquette does not exist[25]. Different services have their own rules of conduct. Such texts in that position may stretch out from ten lines to up to 40 pages. The same applies to the idea of voluntary self-control. The different self-control institutions use various sets of rules of specific content. The efficiency of self-control is unclear as well as its sanction mechanisms cannot be supported by state regulations of enforcement. Beyond contractual obligations, there is no chance to enforce codes of conduct.

In addition, it is still not clear whether the netiquette is conforming to law. The rules might conflict with existing regulations on unfair contract terms and antitrust law. Art. 81 of the Treaty of Amsterdam permit rules of conduct with anti-competitive effects only in so far as such rules repeat and specify existing, EU-conform regulations of unfair competition law. Rules of conduct which restrict a provider's action on the market are therefore dubious under European antitrust law where they restrict an action which subsequently proves to be irrelevant and neutral in the light of unfair competition law.

But the additional question arises whether it is possible to impose sanctions for the violation of codes of conduct. In the United States, the discussion focuses on Alternative Dispute Resolution (ADR) which might lead to the introduction of an Internet jurisdiction and arbitration proceedings in the Internet. However, serious attempts to establish such Internet courts have never been made. And indeed, the introduction of Internet courts would probably not solve the problem of execution, as the decisions of such courts would not be enforceable.

[25] This thesis has extensively been justified by *Hoeren*, in: Becker (Hrsg.), Rechtsprobleme internationaler Datennetze, 1996, pp. 35.

Data Protection and Depersonalisation

The Internet also leads to a depersonalisation of law. All legal rules which relate to a specific "person" have to be reconsidered. People can create new persons, change their identity, and build up virtual realities and virtual entities. For instance, new ways of building up a corporation are establishing in the area of electronic commerce. Virtual corporations are working on a spontaneous, trans-border basis. One of the mayor problems caused by the depersonalisation is the concept of personal data in the context of data protection. Especially, the possibilities of dynamic addresses lead to the question how a concrete person is identifiable via an IP address. Until now, no solution has been found for that problem in data protection law; further research is necessary.

Technology instead of Law

The question therefore arises whether the answer to the machine might be found in the machine itself[26]. A number of difficult legal questions may become obsolete in the Internet by the introduction of certain technical procedures. For instance, in the area of copyright, one has to think of digital watermarking techniques and digital fingerprints[27]. These procedures guarantee that the owner of a right can positively be identified and that cases of piracy can as easily be prosecuted. Reference may also be made for cryptographic procedures[28].

However, the role of technical means within the legal system has to be considered. Technology as such is not more than a fact which per se cannot claim legitimacy. For instance, it would be dangerous to qualify the circumvention of any anti-copying device as illegal. As the anti-copying device could very well be set up by someone who himself is not in the position of a right-holder; the circumvention of security measures which have been established by a software-pirate can not be prohibited. Techni-

[26] See *Hoeren*, Law, Computers and Artificial Intelligence 4 (1995), pp. 175.

[27] *De Selby*, ACM Management Review 1997, pp. 467.

[28] See Imprimatur, The Law and Practice of Digital Encryption, Amsterdam 1998.

cal devices do not create themselves legitimation which causes specific problems in relation to the digital signature[29]. The German *Signaturgesetz* has for instance been praised as it combines very extensive technical standards of certification with a free market economy orientated model of institutions[30]. But this combination is problematic in two aspects. To begin with, the technical security standards have been established so high that hardly any company will be able to meet them. This might just be tolerated in Germany. In an international context however this attempt will be rejected as a discriminating obstruction of access, especially as Germany on its own in the world with these high standards. However, it is not a alternative solution to reduce the value of security standards to zero as it has been done in the EU Signature Directive.

Electronic Commerce and the Problem of Trust

The deciding factor in relation to Electronic Commerce will be the question of trust[317].

Trust in the "Analogous" Environment

Contracts are only concluded by someone who can trust in the performance of the contract by the other party. Such a trust exists if parties are in a long standing business relation and therefore have no doubts concerning the compliance with the contract. However, new connections may contain some difficulties. Apart from problems such as the ability and the willingness to pay, every party has to make sure who the other party is and how the contractual statements of the other party have to be understood. In the "analogous" life, the guarantee of authenticity and identity is given by personal contact or by observance of the written form. If contract negotiations take place in the presence of both parties, either party knows whom one is dealing with and is aware of the content of the declarations of intent. The written form guarantees at least a certain authenticity of the communication; in relation to the declaring person certainty can be reached by introduction of a notary.

Trust and Digital Signature

These trust-building measures will in the long run not be applicable to the Internet. Here, the parties do not know each other; they only meet in the anonymity of the digital world. Personal contacts are missing as much as the possibility to find a safeguard in the written form. Hence, when an electronic order is placed no one knows whether it actually is placed by the person who pretends to be the orderer. The content of an order may also be changed on the long through the Internet to the recipient. In this crisis, asymmetric encoding techniques promise relief. By digital signature they secure the identity and the correctness of the declaring person and protect against undue inspection by encoding with the help of a public key.

But who guarantees that an encoded message really does origin from the person who created the text under a specific name? Here, the German *Signaturgesetz* and the EU Signature Directive refer to the fact that the identity of the sender is guaranteed by the certification authority. In so far this organisation acts a kind of notary. Yet, the certification organisations are governed by private law. Anyone can establish such an institution; according to the draft of the European Commission even without a specific licence. It therefore has to be asked which requirements have to be met in order for the certification institutions to be trusted. It is difficult to create trust via private certification organisations. In this private sector trust can only be created by a security infrastructure which has to be provided by the certification institutions. An advanced level of technology is supposed to create trust.

But this concept has its weaknesses: Trust in technology cannot be created through technology itself. As soon as technology improves, the trust in conventional encoding devices vanishes. Cryptographic methods which are now considered to be safe may soon become obsolete; and then one has to wonder what to do with those keys which have already been distributed. Therefore I think a legislator should not specify the evidential value of a digital signature. As

---

[29] Cf. *Roßnagel*, Neue Juristische Wochenschrift-Computerreport 1994, pp.96; *Bieser*, Computer und Recht 1996, pp.566.

[30] Cf. *Timm*, Datenschutz und Datensicherheit 1997, 525 (528); *Rieß*, Datenschutz und Datensicherheit 1997, 284 (285); *Hohenegg/Tauschek*, Betriebs-Berater 1997, pp. 1541.

[31] See in connection with this *Khare/Rifkin*, Weaving a Web of Trust, in: World Wide Web Journal, Summer 1997, pp. 77.

the digital signature has no established a fixed evidential value; this varies intertemporally[32]. The concept of the European Commission implemented in the Signature Directive is not convincing. According to the Commission, everybody should be able to establish a certification agency without a licence and should only repressively be held responsible via a liability for defects. It is questionable in how far this can establish trust, especially as a certification agency can at any time limit the risk of liability simply by choosing a suitable legal form.

Summary

The previous reflections may be summarised as follows:

1. The Internet does not create net-specific legal problems. Rather, the Internet law itself is only part of the general search for an international information order and the specifications of an information justice.
2. In the information society, a number of new property rights come into existence which cannot be classified within traditional property concepts.
3. The Internet is leading to a dematerialization, deterritorialization, extemporalisation and depersonalisation of law; the legal system thereby loses its traditional (Roman law) roots (person, space, time).
4. Self-regulation in the Internet may assist law, but can never substitute it. Especially questions of antitrust law caused by business self-regulation need of further clarification.
5. Technology can never legitimate technology. Problems of trust in the integrity and authenticity of electronic texts are becoming more and more important.

[32] See in connection with this §§ 17 II, 18 *Signaturverordnung (SigV)*, which came into force on the 1.11.1997.