

Professor Dr. Thomas Hoeren, Münster

Internet and Law - New Paradigms of Information Law

The internet does not - unlike expected - create new legal problems. Some monographs in relation to "cyberlaw" have recently been published. These in particular show that the legal problems of the information law are not quite that new.

And yet, the legal dispute of internet related facts and circumstances gives rise to a number of interesting topoi. Even though they latently existed previously, they only now show their specific explosive effect and diversity.

In the following, I shall try to identify some of these topoi and at the same time outline facets of an independent information law.

I. The Phenomenon of Dematerialization and the new Property Rights

The first striking topoi of the internet law¹ is the net-inherent dematerialization, which leads to a situation where material assets lose their significance in favour of new intangible assets.² Traditionally, the BGB accepts the dichotomy of goods and services.³ 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 a farming to an industrialised society the BGB 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, which are subjected to an independent lawfulness and for which traditional instruments of the civil law cannot provide security.

The Information

First of all, it is a question of information as such⁴. Traditionally, the protection of information is confined to the protection of know-how as it is firmly established in § 17 UWG. This provision is puzzling in a number of ways. To begin with, as a regulation of criminal law it has wrongfully been placed in the UWG. Here the

¹ For the recently published monographs see, for example, *Hilty* (Hrsg.), *Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen*, 1996; *Hoeren/Sieber* (Hrsg.), *Hdb. MultimediaR* (will be published in the near future); *Lehmann* (Hrsg.), *Internet " und MultimediaR (Cyberlaw)*, 1997; *Schwarz* (Hrsg.), *Rechtsfragen des Internet*, Loseblatt (Stand: 1998); *Strömer*, *OnlineR*, 1997; for the austrian law: *Mayer-Schöneberger*, *Das Recht am Info-Highway*, 1997. In the following, due to lack of space, the references shall be reduced to a minimum.

² See *Bercovitz*, *GRURInt* 1996, 1010 (1011).

³ Compare considerations in *Hoeren*, *GRUR* 1997, pp. 866.

⁴ Compare with *Hoeren*, *Information als Gegenstand des Rechts*, *Beil. zu MMR* H. 9/1998, 6*.

legislator's insecurity at the beginning of the century in respect of the exact ratification and protection of information manifests itself. Furthermore, the provision secures the protection of secrets and yet it does so without sufficiently defining the term of "trade secrets".

However, modern efforts to allocate the legal asset "information" are facing very much the same problem. Copyright is cut out for the protection of works of literature and music and until this day has not been adjusted to the needs of a modern information society.⁵ Although the European Commission is trying to initiate such a convergence by establishing a new property right for collections of information⁶ in the European Database Directive⁷, 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 protection of databases as it is laid down in § 87 a UrhG. This symbolises the basic dilemma of information law: definite criteria for the assignment of access to information and exclusive information rights do not exist⁸. The dream of a "Wissensordnung"⁹ remains a dream¹⁰.

The Domain

But other new property rights exist besides the information as such. Their legal fate is unclear. One of these is for example the domain, the marking of a provider's identity in the internet.¹¹ It represents a property asset as long as it labels the virtual

⁵ 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.

⁶ See from the great variety of literature dealing with this topic *Bechtold*, ZUM 1997, pp. 427; *Beger*, GRUR 1997, pp. 169; *Dreier*, GRURInt 1992, pp. 739; *Flehsig*, ZUM 1997, pp. 577; *Gaster*, CR 1997, pp. 660 (Teil I) und pp. 717 (Teil II); *Lehmann*, NJW-CoR 1996, pp. 249; *Wiebe*, CR 1996, pp. 198.

⁷ *Richtlinie 96/9/EG v. 11.3.1996, ABLEG Nr. L 77 v. 27.3.1996, 20 = EWS 1996, 199*. See articles by *Gaster*, who on the part of the European Commission had authoritative influence over the coming into existence of the Database Directive, for example *Gaster*, Ent.LR. 1995, pp. 258, *Gaster*, ÖSGRUM 19 (1996), pp. 15; *Gaster*, *Revue du Marché Unique Européen* 4/1996, pp. 55.

⁸ Compare with the thesis by *Druey*, *Information als Gegenstand des Rechts*, 1995, pp. 441.

⁹ Fundamental *Spinner*, *Die Wissensordnung*, 1994, especially at pp. 111.

¹⁰ 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 identifiable.

¹¹ Compare from recent literature *Bettinger*, GRURInt 1997, pp. 402; *Omsels*,

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 distributing organisations; these \square so to speak- stand 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 \square first come first served \square , 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.¹² Yet, the state refuses to positively intervene with the system of granting domains as favoured by the distributing organisations to the benefit of a third person¹³. That is, the infringer does not have to assign the domain to the person entitled to; he only is under the obligation to discontinue the use of the disputed domain.

But indeed, the identifying power of a domain could be reduced. To begin with, one has to recognise the growing importance of search engines, especially for the virtual identity of the provider¹⁴. 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 \square 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.

GRUR 1997, pp. 328; *Stratmann*, BB 1997, pp. 689; *Ubber*, WRP 1997, pp. 497; *Völker/Weidert*, WRP 1997, pp. 652; *Wilmer*, CR 1997, pp. 562.

¹² 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*, GRURInt 1997, 404 (pp. 420); *Kur*, CR 1997, pp. 325.

¹³ So at least the *Krupp*-decision OLG Hamm, MMR 1998, 214 with comment by *Berlit*, NJW-RR 1998, 909 = NJW CoR 1998, 175 = CR 1998, 241 with comment by *Bettinger*. Of a different opinion for example *LG München I*, NJW-RR 1998, 973, CR 1997, 479; *LG Frankfurt a.M.*, MMR 1998, 151; *LG Düsseldorf*, CR 1998, 174.

¹⁴ See *Wilmer*, CR 1997, pp. 562.

The Internet and the Deterritorialization of the Law

In the internet, all provisions referring to the place, the territory or the seat are faced with nothingness. The electronic speed deterritorialises the law¹⁵.

Problem Areas

To begin with, something to be noticed are the provisions of the law of civil procedure and the conflict of law rules. Due to their origin in the idea of nation states in the 19th century, these provisions very often refer to local connections. This is the case for example 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 consumer 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 permanent establishment¹⁶, which especially in relation to the internet creates almost unsolvable problems.

But also in the law of contracts, territorial connections are very often misleading in relation to the internet. 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 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, territorial connecting factors create problems in relation to claims to compel someone to refrain from acting. These claims are traditionally limited to the prohibition of a specific act in the territory of a specific state; a prohibition to act which takes effect beyond the borders of the territory of a state would not the least be unenforceable for reasons of public international law¹⁷. However, in relation to internet infringements this would result in a situation where the right to forbearance becomes unenforceable because of technical reasons. For it is presently impossible for a provider to exclude the On-line retrieval of an offer by a user from a specific state territory. It is true, in relation to particular domains it is thinkable to bar retrivals. Yet, the multiplicity of standard identification systems makes a selection unrealisable. In the internet it is impossible to define user groups

¹⁵ See *Vief*, *Digitales Geld*, in: Rötzer (Hrsg.), *Digitaler Schein*, 1991, p. 117, 130.

¹⁶ For a general overview/Generally see *Vink, Albarda and others*, in: *Caught in the Web*, 1998, pp. 58; *Lejeune and others*, *European taxation* 1998, pp.2.

¹⁷ Yet, a different view has been adopted in the Netherlands in the *De Corte Geding*-decisions; see in this context *Brinkhof*, *EIPR* 1994, 360; *Gielen/Ebbink*, *EIPR* 1994, 243. However, recently these court decisions(?) have been revised in the unpublished decision of the *Beropsgericht* (Court of Appeal) Den Haag from the 23.4.1998, file reference 97/1296 "Boston scientific.

on a territorial basis; no one knows whether the user behind the address [hoeren@aol.com](mailto: hoeren@aol.com) is from Germany, the USA, or Malaysia. This forces German courts to define restrictive orders in broader terms than legally permissible. The prohibition does not only extend to the possibility of an On-line retrieval in Germany, but also to the entire www-supply, even if this should be legally allowable in other jurisdictions. The KG was the first German court to emphasise this problem and the judiciary's dilemma when rendering restrictive orders. It felt forced to render a second order and to prohibit the www-supply on a world-wide scale¹⁸.

Possible Solutions

The question is indeed how the law should respond to the international 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 business¹⁹. Within this space, providers have to reveal their identity as it is in fact intended by § 6 I MedienStV and § 6 TDG²⁰. This oath of disclosure is only necessary for the assertion of a claim to the right to forbearance in court. For even in the next millennium we will not be able to refrain from asserting claims through state organs of decision-taking and enforcement.

However, what counts otherwise is the virtual activity of the user. In so far, one should abstain from legal provisions which take into account the seat, the place of business or the domicile of the person affected. This avoidance will show its greatest effect where territorial accents have always been favoured: on the conflict of laws and the international law of civil procedure. Here, characteristics of the Cyberspace would best be served by relying on the principle of territoriality as a universal rule for establishing a connecting factor. The principle of territoriality originates from competition law²¹ and defines the scope of state regulations according to the place where the final 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 law²². Furthermore, it shows similarities with the American "minimum-contracts-principle". The dominant opinion has to this day always rejected the application of this principle to intellectual property law by arguing that a jurisdiction could only confer

¹⁸ KG, NJW 1997, 3321 "Concept Concept.

¹⁹ See *Turkle*, *Leben im Netz* 1998, p. 9.

²⁰ See in connection with MedienStV and TDG generally *Bröhl*, CR 1997, pp. 74; *Engel-Flechsig*, ZUM 1997, pp. 234; *Hoeren*, *Jahrb. f. Telekommunikation und Gesellschaft* 1997, pp. 133; *Koch*, NJW-CoR 1997, pp. 302; *Rößnagel*, NVwZ 1998, pp. 1.

²¹ See *BGHZ* 113, 11 (15) = NJW 1991, 1054 "Kauf im Ausland"; *OLG Karlsruhe*, GRUR 1985, 556 (557); *Kotthoff*, CR 1997, pp. 676.

²² *Hilgendorf*, NJW 1997, pp. 1873.

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 jurisdiction²³.

The Internet and the Extemporalization of the Law

But even temporal connections/relations are reduced to absurdity by the internet.

Problem Areas

One provision to be taken into account is § 130 BGB, which provides for a revocation right if the declaration of revocation reaches the recipient at least contemporaneously. In the internet, orders are being completed with such a speed that this revocation right – especially in relation to automated ordering systems – in fact travels dead. Hardly anyone dealing with such a system should be able to formulate a revocation so speedy as that it arrives before or at the same time as the act which is being attacked.

First signs of a detemporalization by the internet can also be found in the law of copyright. In so far, the German intellectual property law has for a considerable time been trying to gain control over the phenomenon of the – successive public – which appears in connection with On-line services. The only intangible way recognised by copyright of using a work is the simultaneous reproduction of it to a number of people²⁴. In so far typical is the broadcasting of television and radio programmes. However, the internet reduces the characteristic of simultaneousness of access to nonsense. Requests are not being made simultaneously but successively. Generally, more often than not the internet is dealing with services on demand, rather than distributing services²⁵. In this situation one could try to apply rules traditionally regulating the public reproduction mutatis mutandis to services on demand. However, this in Germany common way of action has become obsolete by the decision of the international community of states to introduce a new right of – making available to the public – into copyright²⁶. This solves the problem of the categorisation of services on

²³ The different possibilities of solution are discussed in *Hoeren/Thum*, ÖSGRUM 20 (1997), pp. 78. See also BGH, MMR 1998, 35 with comments by *Schricker* "Spielbankaffaire".

²⁴ See *Schricker/v. Ungern-Sternberg*, UrhG, "15 Rdnr.30 with further comments. Of a different opinion only *LG Berlin*, Schulze LGZ 98, 5 (" 11 II LUG), and *öst. OHG* in the Arpanet-decision.

²⁵ For differentiation see *Hoeren*, CR 1996, pp. 517.

²⁶ See Art.8 WIPO Copyright Treaty and based on this Art.3 I, Entwurf zur Richtlinie für eine Harmonisierung bestimmter Aspekte des Urheberrechts und der

demand; holding information for demand already constitutes an infringement of the exploitation rights of the owners of copyright and neighbouring rights²⁷. Yet, there will be problems following from this, such as how to distinguish between public and non-public in the so called *intranet* and the integration of the new intellectual property right into the system of exceptions from copyright.

The phenomenon of lost time does not spare the law of consumer protection. An important instrument of consumer protection is the gain in time to the benefit of the consumer. This protection from over-rushing is predominantly guaranteed by the introduction of the revocation right and the compulsory requirement of the written form (see for example §766 BGB; §4 VerbrKrG)²⁸. Although it quickly showed that the classic team of *Verbraucherkreditgesetz* and *Haustürgeschäftewiderrufsgesetz* in its essence cannot be applied to electronic commerce²⁹. However, the occurring gap in the protection might be closed from the year 2000 onwards by the transformation of the Distance Selling Directive^{30, 31}. Yet, specifically this directive shows the dilemma of electronic commerce in relation to consumer protection. Indeed, 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 wide sections of the www. The problem of time is dealt with even more lax in the discussion concerning the electronic form³². It has almost advanced to the credo of the signature scenery that through the introduction of requirements by the *Signaturgesetz*³³, the digital signature has become the functional equivalent to the hand-written form³⁴. When

verwandten Schutzrechte in der Informationsgesellschaft vom 10.12.1997, KOM (97) 628.

²⁷ See *Lewinski*, MMR 1998, pp. 115.

²⁸ *Kemper*, Verbraucherschutzinstrumente, 1994, pp. 220.

²⁹ *Meents*, Verbraucherschutz und Internet, Diss. Münster 1998; *Waldenberger*, BB 1996, pp. 2365.

³⁰ Richtlinie 97//EG des Europäischen Parlamentes und des Rates v. 20.5.1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz.

³¹ For general information in connection with this directive see *Bodewig*, DZWRiR 1997, pp. 447; *Gößmann*, MMR 1998, pp. 88; *Kröger*, in: *Albarda*, Caught in the Web, 1998, pp. 29; *Martinek*, NJW 1998, 207; *Reich*, EuZW 1997, pp. 581.

³² Compare *Bizer/Hammer*, DuD 1993, pp. 619; *Ebbing*, CR 1996, pp.271; *Heun*, CR 1995, p.2; *Kilian*, DuD 1993, pp. 607; *Pordesch/Nissen*, CR 1995, pp. 562.

³³ The *Signaturgesetz* is part of the *IuKDG*, see BGBl I, 1870. See also *Roßnagel*, NVwZ 1998, 1 (pp. 5); DuD 1997, pp.77; MMR 1998, pp. 75.

³⁴ Of a different opinion: *Erber-Faller*, CR 1996, 375 (pp. 378). The attempt by the *Bundesjustizministerium* to solve the problem of the written form by introducing an electronic text form has failed: see the *Entwurf eines Gesetzes zur Änderung des Bürgerlichen Gesetzbuches und anderer Gesetze vom 31.1.1997* " BMJ 3414/2 (unpublished).

complying with the rather high security standards, a digital signature does indeed perform most functions of the hand-written signature, that of authentication as well as conclusion of contract. However, at the same time the loss of the warning function 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

It shows that through an increasing speed of transmission, legal rules which refer to a temporal delay as authoritative lose their basis. This loss has to be compensated; what is needed is the judicial rediscovery of slowness on a great scale. For example, when substituting the written form for electronic equivalents, the user 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 a content. ¶ 130 BGB has to be replaced by a revocation right of its own nature, 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.

Self-regulation instead of state regulation

The amount of problems surrounding the enforcement of the law result in a growing number of voices calling for self-control and self-regulation in the net. This debate is in a peculiar way connected with an earlier formulated question by Teubner concerning self-regulation³⁵. The debate has basically been settled since the literature reacted with strong criticism to Teubner's different approaches. However, because of the internet, defenders of Teubner's line of thought once again see their chance. In their eyes, the different forms of codes of conduct which are present in the internet confirm their theory that intervention by the state could be replaced by self-regulation. In this context they refer to the so called Netiquette, the manners in the internet, and the different efforts of voluntary self-regulation by providers.

However, only little attention is drawn to the fact that "the" Netiquette does not exist³⁶. Different services have their own rules of conduct. Such texts in that

³⁵ *Teubner*, *Recht als autopoietisches System*, 1989; ARSP 1982, pp. 13. For criticism of *Teubner's* approach see *Habermas*, *Faktizität und Geltung*, 1992, pp. 62; *Tonner*, *KritJ* 18 (1983), pp. 17.

³⁶ This thesis has extensively been justified by *Hoeren*, in: *Becker* (Hrsg.),

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. Unclear is also the efficiency of self-control as its sanction mechanisms cannot be supported by state regulations of enforcement. The attempt to qualify it as a distinguished expression of a code of conduct of a professional group in the meaning of § 1 UWG seems to have failed due to the fact that a homogeneity similar to that of the independent professions is missing in the context of internet-users. Therefore, beyond contractual commitments, a stately enforcement of internet self-control fails. Only when rules of conduct become binding by way of contractual agreement – for example between access provider and user -sanctioning comes into question.

But the remaining question in that case is whether such self-obligations are conformable to the law. This question is of pressing nature especially in relation to the terms control of the AGB-Gesetz. For example, if general terms and conditions of trade prohibit the receipt of advertising by the user it has to be asked whether this is in compliance with § 3 AGB-Gesetz³⁷. Using mailing services in order to demand advertising is lawful -- contrary to case of undesired advertising-mails³⁸; every user can ask to be mailed the advertising he wants. It therefore must be rather astonishing for the internet-user to realise - after agreeing with the provider that he should be provided with a "free pass" for the internet - that the provider denies him to get hold of desired advertising-mails.

Also unclear is the legitimacy of self-control in the context of antitrust law. The deficiency of legitimacy is most obvious in the distribution of domains by the NIC-Organisations³⁹. A state declaration of legitimacy is missing and will not be declared in the future. Instead, these distributing organisations act in a vacuum, which is accordingly also host to the distributed names. Also in relation to codes of conduct - for example in the context of protection of children and young persons - the question to be asked is why private providers specifically are able to establish and control restrictions on a greater scale. GWB and Art. 85 EGV permit rules of conduct with competition restraining content only in so far as such rules repeat and specify existing, EU-conforming unfair competition law. Rules of conduct which restrict a provider's action on the market therefore stand with one foot in the grave of antitrust law. In as far as they restrict an action which subsequently proves to be irrelevant and neutral in the light of unfair competition law, they violate § 1 GWB, respectively Art. 85.

Rechtsprobleme internationaler Datennetze, 1996, pp. 35.

³⁷ See in connection with this also *US District Court for the Eastern District of Pennsylvania*, D.C. Epa, CA No. 96 CV-2486, 9/4/96, *Cyber Promotions v AOL*; see BNA Electronic Information Policy Report 1(1996), 519.

³⁸ See LG *Traunstein*, MMR 1998, 53 = NJW-CoR 1997, 497. Similar by now Ernst, BB 1997, 1057 (1060); *Schnittmann*, DuD 1997, 636 (639); *Schrey/Westerwelle*, BB 1997, Beil. 18, S.17; *Ultsch*, DZWiR 1997, 466 (470); of different opinion only *Reichelsdorfer*, GRUR 1997, pp. 191.

³⁹ See for the related problems of antitrust law: *Nordermann*, NJW 1997, pp.1891.

But also the question concerning the possibility to impose sanctions is problematic. To begin with, it has to be asked how a violation of the netiquette can be sanctioned. In so far as German courts secure compliance via § 1 UWG, enforcement on national level is guaranteed. However, the internet-inherent deterritorialization creates problems of enforcement in relation to foreign countries. If a provider absconds to a foreign country, he can skilfully use this as an enforcement haven in order to avoid any execution of the law. With the failure of state execution, the call for private enforcement according to independent procedural rules becomes louder. What springs to mind is the familiar American discussion of Alternative Dispute Resolutions (ADR). Parallel to this, in the USA one thinks about the introduction of an internet jurisdiction and arbitration proceedings in the internet. However, the discussion has never left the stage of consideration. Serious attempts to establish such virtual decision-taking bodies are not known of. And indeed, the introduction of internet courts would probably not solve the problem of execution, as the decisions of such courts - in contrast to national courts which at least guarantee enforcement on a national level and in the context of international treaties - would not be enforceable. In particular, these are often not arbitration tribunals in the meaning of §§ 1041 ff. ZPO. In addition to this, the decision of an internet court is no longer based upon the common sense of the web community. The community of web-users has changed, to a growing extent it is less homogenous, detaching itself from old times of university research. In the age of electronic commerce the elegant way of ADR is out of question for the internet.

However, gone with this is also the enforcement by technical means. Most heard of is probably the example of mail-bombing, which is often used in the fight against unwanted E-mail-advertising. The user covers the provider with an overwhelming flood of libellous E-mails. This may lead to a situation in which it becomes impossible for the provider to use his internet access as it is overloaded. Yet, it still has to be shown whether such a virtual law of the jungle is in compliance with the prevailing law. For instance, it is extremely difficult to give these sanctions a form which conformable to the law. To call a boycott, in form of mail-bombing for example, is reminiscent of the established case law of the BGH in relation to the boycott-question, in which the BGH qualifies calls for action as an interference with business⁴⁰.

V. Technology instead of Law

The above mentioned facet of the discussion leads to a more fundamental observation: maybe the answer to the machine lays in the machine itself⁴¹. A number of difficult legal questions may become obsolete in the internet by the introduction of certain technical procedures. Here, one has to think of Digital

⁴⁰ Compare *BGH*, DB 1965, 889; NJW 1998, 377.

⁴¹ See in connection with this *Hoeren*, Law, Computers and Artificial Intelligence 4 (1995), pp. 175.

Watermarking Techniques and Digital Fingerprints⁴². These procedures guarantee that the owner of a right can positively be identified and that cases of piracy can as easily be prosecuted. Something similar is true for cryptographic procedures, which especially in connection with the discussion surrounding the digital signature experience an enormous boom⁴³.

However, the question of how these procedures themselves should be positioned within the legal system remains. The technology as such is not more than a fact which from within itself cannot claim legitimacy. In so far 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. The deficiency of legitimation of such technical models becomes particularly apparent in relation to the digital signature⁴⁴. The *Signaturgesetz* has been very much praised as it combines very extensive technical standards of certification with a free market economy orientated model of institutions⁴⁵. But this connection 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. The European Commission will be kept on its toes by this circumstance. As long as there is no market model for certification institutions which would be acceptable throughout Europe, the future of the *Signaturgesetz* is uncertain.

The model of institutions as favoured in the *Signaturgesetz* proves to be even more problematic. The assignment of certifying functions to bodies governed by private law has already been criticised in relation to electronic commerce; this almost wrecked the *Signaturgesetz* in the *Bundesrat*⁴⁶. However, detached from this question has as yet the applicability of the *Signaturgesetz* to the field of public administration not been considered. In the future it will be possible for a private business to certify the issuing of a driving licence or to authenticate the making out of an order imposing punishment by a public authority. From my point of view this is very problematic. Until now public administration gained its authority solely from within itself, the identity of the issuing authority of an administrative act was only verified within the system of administrative organisation law. However, in the digital context private bodies (partially) authenticate the validity of jurisdictional orders; quelle surprise.

VI. Electronic Commerce and the Problem of Trust

⁴² *De Selby*, ACM Management Review 1997, pp. 467.

⁴³ See *Imprimatur*, The Law and Practice of Digital Encryption, Amsterdam 1998.

⁴⁴ *Roßnagel*, NJW-CoR 1994, pp.96; *Bieser*, CR 1996, pp.566.

⁴⁵ Compare *Timm*, DuD 1997, 525 (528); *Rieß*, DuD 1997, 284 (285);

Hohenegg/Tauschek, BB 1997, pp. 1541.

⁴⁶ See BT-Dr 13/73885, pp.57 and BR-Dr 420/97.

The deciding factor in relation to Electronic Commerce will be the question of trust⁴⁷.

1. 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 will to pay, every party has to make sure who the other party is and how the other side's declaration has 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 (§ 147 I BGB). 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 (§§ 128, 129 BGB).

2. 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, only meet in the digital environment. 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 intercepted and 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 originate from the person who created the text under a specific name? Here, the *Signaturgesetz* refers to the fact that the identity of the sender is guaranteed by the certification organisation (§ 5 I Signaturgesetz). In so far as it takes over the function of the notary. Yet, the certification organisations are governed by private law. Anyone can found such an institution; according to new plans by 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 has already been mentioned that such trust is stretched to its limits where the exercise of jurisdiction is certified by private agencies. For the private sector of the economy the problem of trust is solved by a security infrastructure which has to be provided by the certification institutions. An advanced level of technology is supposed to have trust inspiring

⁴⁷ See in connection with this Khare/Rifkin, *Weaving a Web of Trust*, in: *World Wide Web Journal*, Summer 1997, pp. 77.

effect. It shall also guarantee the unmistakable allocation of a key to one specific person and that data for certificates can not be changed unnoticed.

But this procedure has its weaknesses: to begin with, the high security standards are seen by some European states as exaggerated and are rejected by the European Commission for being anti-competitive. In so far, the level of security will be lowered throughout Europe, which will give rise again to the question of trust. Secondly, methodologically the trust in technology cannot not be justified 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 the legislator has come to the right conclusion in not specifying the evidential value of a digital signature. Because the digital signature has no established evidential value; this varies intertemporally⁴⁸.

Hence, one should resort to real and expert evidence in order to make clear from case to case which influence the respective procedures have on the evidential value of a digitally generated and transmitted document⁴⁹. Attention has also to be drawn to the question of identity in relation to the certification organisations themselves. Reference can only be made to the basic certificate of the regulating authority, which holds the "meta-key" so to speak (¶ 4). The public key of the regulating authority itself is published in the *Bundesanzeiger* in order to guarantee its integrity. This shows that once again at the end of the certification chain stands the good old paper. But this nostalgic outlook is deceptive as the European Commission plans the complete dispensation with any key-hierarchy⁵⁰. 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.

VII. Summary

The previous reflections may be summarised as follows:

1. The internet does not create net-specific legal problems. Rather, the internet itself is no more than the top of the iceberg of the general search for an order of knowledge and the specifications of an information justice. Behind the internet arches the zenith of the information law.

⁴⁸ See in connection with this "" 17 II, 18 *Signaturverordnung (SigV)*, which came into force on the 1.11.1997.

⁴⁹ In so far even more surprising is the fact that the Italian law accepts digital signatures as a proper equivalent to signatures under paper documents.

⁵⁰ See the joint proposal of the European Parliament and Council in relation to outline conditions for electronic signatures of the 13.5.1998, KOM (1998) 297. For a summarising presentation of the draft see MMR 6/1998, with comments by *Roßnagel* and *Gleis*.

2. In the often conjured information society, a number of new property rights come into existence which escape a legal qualification according to previous attempts of classification. Two of these new property rights are the information and (as yet) the domain.
3. The internet introduces a dematerialization, deterritorialization and extemporalisation of the law and by this loses its substrates which were inherited from the Roman law (asset, space, time). Into the gap steps the virtual "space" and the discovery of slowness.
4. Self-regulation in the internet may complete the law, but can never substitute it. Especially questions of antitrust law surrounding the enforcement of private rules of conduct are in need of a more detailed clarification.
5. Technology can never legitimate technology. It follows that the problem of trust in the integrity and authenticity of electronic texts proves to be almost unsolvable.