2. Current developments

2.1. Repersonalisation

The legal system has understood that it cannot tolerate the depersonalised effects of the network. This is because there would be no liability without a tangible person. If it is impossible to get hold of the person directly responsible, it is necessary to find intermediary liability. Only with this in mind we can understand the strong attitude of the courts towards the responsibility of the *Admin-C (administrative contact)*[1]. The DeNIC has introduced the Admin-C in order to have a service official according to §§ 174 f. ZPO (German Civil Procedure Code) in case that a domain holder is established abroad. The jurisdiction has started to establish the responsibility of the Admin-C not only for violation of trademarks[2] but also for violation of competition law[3] in the absence of access to a domain holder. For such liability, it should be sufficient that someone has wilfully and by adequate cause contributed to the causing or maintaining of an unlawful impairment of another person regardless of fault[4]. I don't want to raise the question of whether this construction is justifiable. My interest lies in identifying – in the sense of an empirical result – that for the first time, a repersonalisation of the internet can be traced. This movement was intensified by the principles of the BGH's judicature in the Rolex-cases. Intermediates like online auction websites, link setters and licensees of forums become victims of action for an injunction by disregarding the facilitation of liability because of the E-Commerce-directive[5]. The repersonalisation however begins in other parts of law. One may be

---

[1] KG Berlin (Higher Court Berlin), MMR 2006, magazine 6, 392 = CR 2006, 778 = ZUM 2006, 461; critically OLG Hamburg (Higher Regional Court Hamburg), MMR 2007, magazine 9, 601 = BeckRS 2007, 10375 = ZUM 2007, 658; LG Bonn (District Court Bonn), verdict of 23 February 2005 – 5 S 197/04 CR 2005, 527; Hoeren, Eustergerling (2006), p. 132.

[2] OLG Stuttgart, MMR 2004, magazine 1, 38, 39 = CR 2004, 133 = K&R 2004, 599; Stadler (2004), p. 521.

[3] In favor of a restrictive applicable liability of the Admin-C: LG Dresden, MMR 2007, magazine 6, 394 = CR 2007, 462, agreeing: Wimmers, Schulz (2007), p. 463.

[4] Cf. BGH (Federal Court of Justice), NJW 2004, 3102 = BGHZ 158, 236 = CR 2004, 764 = JZ 2005, 33 = ZUM 2004, 831 = MMR 2004, 668 w. comment Hoeren; BGH, NJW 2001, 3265 = MMR 20011, 671 – ambiente.de. Those principals are applicable according to §§ 823 I, 1004 BGB (BGH, NJW 2004, 3102 = MMR 2004, 668 w. comment Hoeren; KG Berlin, verdict of 10 February 2006 – 9 U 55/05 = MMR 2006, 393 w. comment Spieker – in this magazine).

[5] BGH, ZUM 2007, 846 = AfP 2007, 477 = CR 2007, 728 = GRUR 2007, 890; discussion on this: Döring (2007), p. 1131; also: Leible (2007), p. 3324.

surprised by the consequent manner in which the judicature punishes infringements against the obligation of a site notice. But the specific duties of identification by the TMG (German Code of Tele-Media) or the BGB-InfoVO (by-law to the German Civil Code) are also used for grasping a real person and the corresponding data which should be contained in a site notice. Furthermore, the movement corresponds to the behaviour of young people in the Web 2.0. Young people pay homage to their own personality with such hypertrophy – a virtual exhibitionism – through the striptease of personal data occurring by users of studiVZ and other social networks.

In contrast to this development and contrary to expectations, the old aspects of depersonalisation, which were emphasised 10 years ago, did not become relevant. Virtual companies-an 'in' expression of the first internet-hype – have never gained importance. Anonymizers have left the internet unsung-also as a result of pressure exercised by the legal profession. In the time of the second internet-hype virtual communities – like Second Life or World of Warcraft – won a lot of popularity, nowadays hardly anybody is talking about this phenomenon anymore.

2.2. Reformalisation

The predicted movement to a deformalisation of law did not become reality either. Indeed, regulations which tie in to the written form are obsolete in the virtual context. Nevertheless, alternative requirements have taken of the written form. It is to be regretted again that the "qualified signature" did not become of relevance; it has never really found acceptance in Germany over the past years and probably never will. The text form according to § 126 BGB (German Civil Code) has taken the place of the written form. The key characteristic of the text form is the requirement of a permanent rendition of characters. According to the legendary ruling of the Kammergericht Berlin (Regional Appellate Court of Berlin) concerning § 312c I 1 BGB[6], this requirement is only fulfilled if the consumer actually perpetuates his declaration by printing it out or saving it to his hard drive. This can lead to great difficulties in practice, in particular concerning the informational obligations with regard to internet auction transactions. Thus, in practice, good old-fashioned paper is still of importance[7]. The internet has not actually lead to a reduction in the amount of paper used; in fact, much more is printed out. This also results from provisions set by lawmakers. The decisions of the OLG (Higher

[6] KG Berlin, NJW 2006, magazine 44, 3215 = MMR 2006, magazine 10, 678; subsequent: KG Berlin, MMR 2007, magazine 3, 185.

[7] OLG Köln, MMR 2007, magazine 11, 713; more elaborately: Bonke (2006), p. 3169.

The phenomena of deterritorialisation have been much attested to since the beginning of the development of the internet[14]. In the early 90's David Johnson and David Post began to glorify the infinity of the web as the ideal of a new internet state. Many people followed suit and conjured up a dream of the internet as a legal vacuum, talking about a legitimation crisis and a deconstruction of the national state[15]. Oases of legality and the lack of enforceability of national judicial acts in third states were quickly pointed out[16]. The bubble burst – and at a very early stage – as a consequence of the reflections of the French judge Gomez on the Yahoo! – case[17]. For the first time worldwide, the French justice granted a kind of reterritoiralisation of the internet, meaning a territorial restriction of the access to a webpage. Judge Gomez based his ruling on a report written by two Frenchmen and the American Co-founder of the Internet, Vinton Cerf. According to their report, it could be ensured up to 70 % that the French webpages in question could no longer be accessed because the user could be localized via his IP-address. Based on these findings in the report, Gomez ruled that Yahoo! could put corresponding IP-barriers in place in relation to the French user. Yahoo! was very much against this concept and argued that an IP-localization was impossible or disproportionally complex to say the least. Thereupon, US-courts refused to enforce the French ruling. However, the question of IP-identification and its validity remains unanswered. This is especially precarious because such an identification process could solve a lot of the problems arising from a conflict of laws in the internet. If it were possible to restrict access to websites territorially, the target direction and market location of a website could also be designated. This specification would then again have to be considered with regard to a conflict of laws in the sense that the construction of a website would no longer have to succumb to the law of all states, but to the legislation of the respective designated target state only.

This gave rise to the discussions about *Zoning* and *Geolocation*[18]. Today, these methods are well-established. They are used by states such as China as means of controlling the internet, but also as protection against spam and phishing. The current methods gear to the regional specifications of IP-addresses or IP-areas. The current hit rate lies at around 90-98 %. Hence with Geolocation, a service has actually been provided with which territorial borders can be displayed on the web.

---

[14] Cf. Johnson, Post (1996a); Johnson, Post (1996b); Burk (1997).
[15] Cf. Castells (2003a), p. 286ff. and Castells (2003b), p. 379ff.
[16] Cf. Hoppmann (1999), p. 673.
[17] English version: http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm.
[18] Hoeren (2007), p. 3.

Appellate Court) Köln[8] and Hamburg[9], which have defined the value of electronic documents as evidence in court as very low, are still leading cases today. Therefore, when in doubt, internet providers continue to use paper to document their contracts and other declarations[10]. Worth mentioning in this context is also the "own goal" shot by tax legislation concerning input tax deduction with electronic invoices. According to § 14 UStG (German Purchase Tax Code) the authenticity of origin and the integrity of the content must be certified by a *qualified electronic signature*[11]. For lack of such a signature, the former senders of electronic invoices are choosing the easy way out: on the basis of EDI-Regulations in § 14 UstG paper invoices are sent out on a monthly or yearly basis, which are intended to "degrade" the previously sent electronic bills to mere "interim bills"[12]. Thus, the question of form oscillates between text form and written form in negligence of a qualified signature.

In any case, the intended warning function of the text form has been assumed by another instrument – the obligations to inform and clarify. These obligations have rapidly increased in number in recent years, as a result of European provisions. Meanwhile, every website has to contain up to 20 informational details; if consumers are involved, websites may carry up to 100 specifications[13]. Many of the obligations to inform have replaced the old written form requirement. For example, the consumer is to be informed about the different technical steps leading to a contract (§ 3 nr. 1 BGB-InfoVO). The so-called "about" or "legal information" – obligation is another example of an obligation which serves to fulfil the warning function; the user of a website should know whom he is dealing with.

2.3. Reterritorialisation

---

[8] OLG Köln, CR 2003, 55 = K&R 2003, 83, w. confirming comment Roßnagel; LG Bonn, MMR 2002, magazine 4, 255 = CR 2002, 293, w. confirming comment Hoeren; LG Konstanz, MMR 2002, magazine 12, 835 = CR 2002, 609; LG Erfurt, MMR 2002, 127.

[9] OLG Hamburg, MMR 2002, magazine 12, 821.

[10] Concerning proof of receipt when using fax, e.g.: KG Berlin NJW 1994, 3172f; OLG Dresden, NJW-RR 1994, 1485; OLG Köln, NJW 1995, 1228; BGH, NJW 1995, 665ff; AG Köln, RDV 1999, 32; in summary Henneke (1998), p. 2194f, p. 2958; Töperwin (1999), p. 241ff.

[11] Purchase tax directives 2008, Nr 184a; re qualified signature: Roßnagel (2007), p. 1233.

[12] AG Hamburg-Altona: StBgebV: DStrV 2006, magazine 34, 1523; AG Brühl, verdict of 12 April 2006 – 21 C 612/05 = BeckRS 2007, 14273.

[13] Concerning the obligations to inform and pricing specifications: BGH, BB 2008, 74, w. comment Hullen.

However, it should be noted that means of circumventing the process do exist and that there is a need for a constant update of the IP-databases.

3. Aporia

With a view to legal decision-making however, the prospects of reterritorialisation, repersonalisation and reformalisation lead to an aporia. As explained below, legal thinking is based on a forensic necessity for clear "yes or no answers". Technical questions on the other hand often lead to statements of probability. *Statements of probability* are quantified statements about the probable reliability of partial systems in relation to the types and processes of malfunction of its components[19]. These statements are lacking the binary judgement "yes" or "no"; the question asked here in fact is if and to what degree an event is more or less likely to occur rather than its alternative. Legal cases concerning the internet are often characterised by considerations of probability.

3.1. Probabilism: Examples

Concerning reterritorialisation, for example, problems arise in respect to Geolocation. This is because with zoning, the user can - by adeptly choosing the IP-address- undermine an IP-scan and thus make a territorial allocation impossible. Hence Geolocation only allows for a probable allocation of IP-address and territory. Unwanted discrepancies can also occur with reterritorialisation, especially concerning liability law. With the ruling of the LG Hamburg[20] the question arises as to whether the not improbable possibility of misuse of wi-fi-connections leads to an obligation to check and act. In its "Use-net" ruling, the LG Munich I[21] - like many other courts - pointed out that concerning the legal obligations of cache providers to check, it is necessary to differentiate according to the particularities and necessities of each case and to the technical and economical effort involved. With regard to reformalisation, the standard of evidence of electronic documents (apart from the qualified digital signature) can only be considered according to § 286 ZPO. The

---

[19] Cf. Winter, Schäfer (1985), p. 703.
[20] LG Hamburg, MMR 2006, magazine 11, 763 = CR 2007, 54 = ZUM-RD 2006, 533.
[21] LG Munich I, MMR 2007, magazine 7, 453 = ZUM 2007, 496; also: LG Düsseldorf, MMR 2007, magazine 8, 534.

judge can only set the value or standard of evidence according to his own free consideration. This means that statements regarding the value of evidence can only be made via probability criteria.

3.2. Legal Logic

The legal profession has its difficulties with statements of probability[22]. Law has a binary coding– either something is forbidden, or it is not[23]. Therefore, since the development of internet law, the legal field has tried to ensure the transformation of probabilities into the binary logic of the jurisprudence. The solution cannot be found by looking at the law of technology, where these transformational problems have been well–known for quite some time[24]. To this end, the linkage required between the law of technology and the law of information does not exist worldwide, even though much could have been learnt from the former discussion about risk management, for example, concerning nuclear law[25]. Information law is too wide–reaching and omnipresent for it to be linked with the highly complex law of technology, which is restricted to the experience of very few experts. The solutions of information law were, and are still, much more ambivalent and complex than those of the law of technology.

3.3. Methods of resolution

The solutions of the legal profession are complex.

3.3.1 Shift to authorised experts

One option which is common with the law of technology is the shifting of governing power to authorised experts. This can be done by shifting proceduralisation, i.e. the integration of proceeding competent bodies. In fact, in the early days of the internet

---

[22] Cf. Schmidt (1972), in particular p. 163–178 and in the law of administrative proceedings: Nell (1982), p. 93ff, p. 209ff.

[23] Generally: Luhmann (1991), p. 61ff; critically Meder (1993), p. 265ff; Damm (1999), p. 93, 112.

[24] Concerning the importance of technical rules in liability and insurance law, see Marburger (1983), p. 597.

[25] For example, cf. re compulsory cover for clinical tests using radioactive substances and ioinised rays: Taupitz, Krpic–Mocilar (2003), p.533.

the dream of self-control, co-regulation, regulated self-regulation was dreamt. However, Netiquette and RFCs are of as little importance as the Global Business Dialogue and the Tunis-discussion. Furthermore, the authorised expert can also be called upon ex post as the main figure in the process of deciding a case. This is common in IT-law: the authorised expert does in fact often take the place of the judge. The same can be said in conjunction with the standard of evidence of EC/debit-cards[26]. However, the scenario regarding internet law is a totally different one. In the early stages of the internet, cases where authorised experts were integrated existed, albeit only concerning criminal internet law. Worth mentioning in this context is the CompuServe-case[27] or the criminal proceedings against Angela Marquardt due to the Radikal-Links[28]. This integration is not common in civil law however. The judges' expertise tends to substitute that of the authorised experts[29]. The judges of the OLG Hamburg for example hold that they have an excellent knowledge of the usage of graphic Windows-surfaces in the 90's[30]. The judges of the OLG Munich[31] believe to be of sufficient competence to know that an averagely attentive, informed and knowledgeable internet user would assume that "rechtsanwaelte-dachau.de" does not stand for the office of a single lawyer, but for a local registry of all lawyers in the Dachau area. In Cologne[32] one is certain that the possibility of internet access in exchange for a fixed monthly rate without further costs arising was already in discussion as far back as 1999.

In 2006, the BGH[33] finally sounded a note of caution. The Court ruled that generally speaking, it is within the competency of the judge involved to decide whether his expertise is sufficient to allow him to refrain from taking in an authorised expert. However, according to the Court, the judge's discretion has to end where a case requires special knowledge of computer technology. Here the competent judge may only refrain from obtaining expert advice if he can verify that he has the necessary expertise himself. The reference to computer-technical knowledge is treacherous however: the Court refers only to the technical side of the internet regarding data processing, but not to the other particulars of the web

---

[26] BGH, MMR 2004, 812 = NJW 2004, 3623 = Jus 2005, 117.
[27] AG Munich, MMR 1998, magazine 8, 429.
[28] AG Munich, MMR 1998, magazine 1, 49.
[29] To view the few exceptions: OLG Munich, MMR 2001, magazine 6, 375 = NJW 2001, 3553 = GRUR 2001, 499.
[30] OLG Hamburg, NJOZ 2005, magazine 42, 4335 = GRUR-RR 2006, 130 = ZUM 2005, 833.
[31] OLG Munich, MMR 2002, 614 = NJW 2002, 2113 = CR 2002, 757.
[32] OLG Cologne, MMR 2002, 389.
[33] BGH, NJW-RR 2007, 357 = MMR 2007, 178 = CR 2007, 235.

and its users. Accordingly the Court ruled against a particular, internet-specific model consumer in the Epson-decision[34]. At the same time, the 1st Senate for Civil Law claims to know the practices of the internet, for example that a lower entry-level/introductory price on E-bay is a sign for brand piracy[35] or that an electronic press-archive cannot be compiled with PDF-files[36].

3.3.2 Shift to the judiciary

Apart from the inclusion of certified experts, one can usually only resort to *decisionism.* As early as 1995, Lawrence Lessig[37] described the phenomenon of increasing delegation of internet governance to the courts and saw this as a triumphant success and an affirmation of the US case-law-approach. In the time following, Lessig was proven to be correct with regard to the situation in Europe as well. Even aside from the typically case-orientated advertising law, the power of court decisions concerning internet cases was greatly increased during the last ten years. This is due to the fact that legislators have used vague and indefinite legal terms, hence giving the courts the power of decision. In this context, one should recall the claim of the originator to adequate consideration according to §§ 32, 32a UrhG (German Copyright Act), to be determined according to the honest practice of the trade. § 87a UrhG defines the cover amount for databases according to the quantity or quality of relevant investments. The judge's scope for decision is most striking with the law of online marketing, for instance concerning the introduction of new cases of interdiction in the Unfair Competition Law (UWG) or the assessment of the relevancy of an infringement of competition. With regard to the value of proof of electronic documents one can refer to the general principle of the judge's freedom of decision (§ 286 ZPO). Since the Rolex I-decision tort law lacks real contours; as the BGH put behind the legislator's will concerning the far going exemption from liability of Host-, Cache- or Access-Providers. In injunction cases about the liability of troublemakers the decisional prerogative has been given completely to the courts. Since that time, the single elements of the troublemaker liability - the question of reasonableness and proportionality of the existing obligations to examine - are decided differently by each court. The dangers of such a development are obvious albeit they just now have become clear. A competition between the courts is the result, it is a competition about competences and cases,

---

[34] BGH, GRUR 2005, magazine 5, 438.
[35] BGH, NJW 2004, 3102, 3105.
[36] Press release Nr. 76/2002 to the Court's ruling concerning electronic press reviews.
[37] Cf. Lessig (1995).

lead by smart lawyers who know they should go to Braunschweig in case of GoogleAds and to Hamburg when their case is about the Host-Provider-prohibition. Incidentally, courts can only be active ex post and with considerable delay. This leads to dysfunctional effects in the fast developing internet, for instance, a court decision about the admissibility of Metatags can only be reached when search engines have already stopped to count on Meta-technologies.

3.3.3 Solution on the enforcement level

Another solution to the probabilism problem can be found in the Rolex II-decision of the BGH. In this case the First Civil Senate of the BGH has shifted the question of probable efficiency of filtering measures to the level of enforcement. The Court proposes to clarify the question of reasonableness of filtering procedures and the potentially following manual control during enforcement procedure[38]. In the Rolex-I-decision the Senate also emphasises that in case of a conviction to omission the responsible person can only be liable if he meets fault (§ 890 ZPO). In case of infringements that have not been foreseeable in the anticipated filtering procedure he does not meet the required fault[39]. Simultaneously, the OLG Munich has pointed out – as a restriction to omission claims according to insufficient filtering – that in case of potential contravention to the pronounced conviction the responsible person is only liable if he meets fault[40].

This solution is not convincing. § 890 ZPO includes sharp sanctions similar to criminal ones in case of contravention. These are only justified if the debtor can actually recognise in the injunction itself what he is made to do. Even from the perspective of the injunction creditor the shift is more a barrier than benefit; the debtor will be exempted from liability because of lacking fault if he has understood an ambiguous omission order in a justifiable way that excludes the contravention[41]. These problems have early been discussed in context to the European Law on equal treatment[42]. Incidentally, an enforcement court will never be able to pursue an omission claim as intensively as the trial court usually can during main procedure. In my capacity as a judge I have never heard, for instance, that an enforcement court took evidence to clarify the extent of an omission request.

---

[38] BGH, MMR 2007, 507.
[39] BGH, MMR 2004, 668 = NJW 2004, 3102 = GRUR 2004, 860 = ZUM 2004, 831.
[40] OLG Munich, MMR 2006, magazine 11, 739.
[41] Cf. Thomas, Putzo (2007) § 890 margin no. 15.
[42] Cf. Spindler (2001), p. 737; Spindler (2002), p. 921, p. 925.

3.3.4 Solution through prima facie evidence

In dire need the courts fall back on explicit or implicit rules on the burden of proof, especially on unspoken assumptions on the prima facie evidence. Basically speaking, in the procedural practice the Internet Law is a right of prima facie evidence. Insecure WLAN-accounts are typically dangerous. Those who run a forum in the internet have to assume that it will be typically misused. An e-mail is typically sent from the sender that is called in the header and the content of that message is typically showed correctly[43]. Usenet and P2P are typically services for film and music pirates. Such a renaissance of the prima facie evidence even inspires the legislator: the rule on data retention implicitly contains a general suspicion of the entire population; people who talk via mobile phone or surf through the internet are under (even if it is only a vague) suspicion of being a terrorist.

4. Outlooks

What does all this mean to the Information Law Research? So far it has been at the beck of a legislation that reacts to fast key stimuli but that had to consider legal arbitrary postulates far from any systematic or dogmatic. As a reflex to that, some kind of patchwork research and literature developed fixed by compilation and eclectic look on individual laws whose scientific outcome has always been low. Research desiderata are meta-examinations that accentuate the systematic, dogmatic and scientific relation of the Internet Law. Topics as the search for informational justice[44], the relation of Intellectual Property Law and general Civil Law, the establishment of a general part of Intellectual Property Law[45] or the analysis of techno-legal issues are demanded. If such a basic research begins will soon recognize how truly false some "wisdoms" of the information society are. An example is the phrase of Reis: "Horses do not eat cucumber salad." This phrase is false. Horses do eat cucumber salad; it is a well known remedy in veterinary medicine against mouth infections.

---

[43] Cf. Mankowski (2002), p. 2822; in contrast Rossnagel, Pfitzmann (2003), p. 1209; see also Spindler (2008), p. 7.

[44] Cf. Hoeren (2008), p. 3ff; see also Kloepfer (2002), § 4 margin no. 15 ff.

[45] Cf. Ahrens (2006), p. 617.

Bibliography

Ahrens, H.-J. (2006), Brauchen wir einen Allgemeinen Teil der Rechte des Geistigen Eigentums?, in: Gewerblicher Rechtsschutz und Urheberrecht, 2006, p. 617-625.

Bonke, J. (2006), Die Widerrufsfrist bei eBay-Auktionen, in: Neue juristische Wochenzeitschrift, 2006, p. 3169-3173.

Burk, D. (1997), Jurisdiction in a World Without Borders, in VIRGINIA JOURNAL of LAW and TECHNOLOGY, on the WWW under: http://vjolt.student.virginia.edu/graphics/voll/home_art3.html (31.01.2008).

Castells, M. (2002), Die macht der Identität, Opladen 2003.

Castells, M. (2003) Jahrtausendwende, Opladen 2003.

Damm, R. (1999), Rechtliche Risikoverteilung aus zivilrechtlicher Sicht, in: Rechtliches Risikomanagement, Hrsg.: A. Bora, Berlin 1999, p. 93, 112f.

Döring, R. (2007), Die Haftung für eine Mitwirkung an Wettbewerbsverstößen nach der Entscheidung des BGH „ Jugendgefährdende Medien bei eBay", in: Wettbewerb in Recht und Praxis, 2007, p. 1131-1141.

Henneke, S. (1998), Form- und Fristfragen beim Telefax, in: Neue Juristische Wochenzeitschrift, 1998, p. 2194-2195, p. 2958-2959.

Hoeren, T. (1998), Internet und Recht - Neue Paradigmen des Informationsrechts, in: Neue Juristische Wochenzeitschrift, 1998, p. 2949-2854.

Hoeren, T. (2007), Zoning und Geolocation - Technische Ansätze zu einer Reterritorialisierung des Internet, in: Multimedia und Recht, 2006, p. 3-6.

Hoeren, T. (2008), 10 Jahre MMR - eine subjektive Rückschau, in: Multimedia und Recht, 2008, S. 3-6.

Hoeren, T., Eustergerling, S. (2006), Die Haftung des Admin-C - Ein kritischer Blick auf die Rechtsprechung, in: Multimedia und Recht, 2006, p. 132-138.

Hoppmann, C. (1999), Der Vorschlag für eine Fernabsatzrichtlinie für Finanzdienstleistungen, in: Versicherungsrecht, 1999, p. 673-682.

Johnson, D., Post, D. (1996), And How Shell the Net Be Governed?, in: Cyberspace Law Institute, on the WWW under: http::://www.cli.org/emdraft.html (31.01.2008).

Johnson, D., Post, D. (1996), Law And Borders - The Rise of Law in Cyberspace, in: Stanford Law Review, 48 Jg., 1996, p. 1367-1391.

Kloepfer, M. (2002), Informationsrecht, Munich 2002.

Leible, S. (2007), Haftung von Internetauktionshäusern - reloaded, in: Neue Juristische Wochenzeitschrift, 2007, p. 3324-3326.

Lessing, L. (1995), The Path of Cyberlaw, in: Yale Law Yournal, Vol. 104, 1995, p. 1743-1755.

Luhmann, N. (1991), Soziologie des Risikos, Berlin 1991.

Mankowski, P. (2002), Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?, in: Neue Juristische Wochenzeitschrift, 2002, p. 2822-2828.

Marburger, P. (1983), Die haftungs- und versicherungsrechtliche Bedeutung technischer Regeln, in: Versicherungsrecht, 1983, p. 597-608.

Meder, S. (1993), Schuld, Zufall, Risiko, Frankfurt 1993.

Nell, L. (1983), Wahrscheinlichkeitsurteile in juristischen Entscheidungen, Bayreuth 1983.

Roßnagel, A. (2003), E-Mail als Augenscheinsbeweis?, in: Kommunikation und Recht, 2003, p. 84-86.

Roßnagel, A. (2007), Fremdsignierung elektronischer Rechnungen: Vorsteuerabzug gefährdet, in: Betriebs-Berater, 2007, p. 1233-1237.

Roßnagel, A., Pfitzmann, A. (2003), Der Beweiswert von E-Mail, in: Neue Juristische Wochenzeitschrift, 2003, p. 1209-1214.

Schmidt, J. (1972), Teilbarkeit und Unteilbarkeit des Geständnisses im Zivilprozess, Berlin 1972, particularly p. 163-178.

Spindler, G. (2001), Das Gesetz zum elektronischen Geschäftsverkehr - Verantwortlichkeit der Diensteanbieter und Herkunftslandprinzip, in: Neue Juristische Wochenzeitschrift, 2002, p. 921-927.

Spindler, G. (2001), Die zivilrechtliche Verantwortlichkeit von Internetauktionshäusern - Haftung für automatisch registrierte und publizierte Inhalte?, in: Multimedia und Recht, 2001, p. 737-743.

Spindler, G. (2008), IT-Sicherheit - Rechtliche Defizite und rechtspolitische Alternativen, in: Multimedia und Recht, 2008, p. 7-13.

Stadler, T. (2004), Haftung des Admin-C und des Tech-C, in: Computer und Recht, 2004, p. 521-527.

Taupitz, J. Krpic-Mocilar, T. (2003), Deckungsvorsorge bei klinischen Prüfungen unter Anwendung radioaktiver Stoffe oder ionisierender Strahlung, in: Versicherungsrecht, 2003, p. 533-540.

Thomas, H., Putzo, H. (2007), Zivilprozessordnung, 28th edition, Munich 2007, § 890 ZPO, margin no. 15.

Töpperwin, E. (1999), Rechtsfragen rund ums Telefax, in: Deutscher Richterbund, 1999, p. 241-246.

Wimmers, J., Schulz, C. (2007), Zur Haftung des admin-c für unter der URL erreichbare wettbewerbswidrige Inhalte, in: Computer und Recht, 2007, p. 463-465.

Winter, G., Schäfer, R. (1985), Zur richterlichen Rezeption natur- und ingenieurwissenschaftlicher Voraussagen über komplexe technische Systeme am Beispiel von Kernkraftwerken, in: Neue Zeitschrift für Verwaltungsrecht, 1985, p. 703-711.