Articles

Toward a Network-Oriented Law of the Internet! The Necessity to Find a New Balance between Risk and Opportunity in Network Communication

Karl-Heinz Ladeur[*]

A. Preliminary Remarks

This article looks at the reasons for the lack of a discussion on ”network oriented“ media and internet law. The Internet has fundamentally changed the conditions of communication.[1] It has broken down or undermined all borders between formats, individual and mass communication, communication content, and technologies of telecommunication. As a ”network of networks,”[2] it is also a challenge for the legal system which has linked its conceptions and doctrine to those separations and borderlines.

The internet community tends to react to this evolution by a principled opposition to any legal intervention into internet communication which it regards as incompatible with the autonomy of its users.[3] This is, at least in some respect, due to the fear that the new ”relational rationality“ of the net may not only raise the number of choices for the users but also for external control which is simplified by the flexible technology of the internet (whereas at the same time this allows for a reaction to escape or curb control strategies). Certainly the internet is “completely different,“ but this does not exclude the possibility to develop a “completely different“ *legal ordering* which pays tribute to its flexibility and creativity.[4] In the following, with a view to several domains of conflict, it shall be tested

[*] University Professor of Law Emeritus, University of Hamburg Faculty of Law. Bremen Research Professor, University of Bremen, Bremen Graduate School in the Social Sciences [BIGSSS]. Email: karl-heinz.ladeur@jura.uni-hamburg.de

[1] See YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006); CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATION (2009); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2006), who describe the new logic of the internet as not only a new means of communication.

[2] ELIE NOAM, INTERCONNECTING THE NETWORK OF NETWORKS (2001).

[3] For the ideology of this movement see the homepage of the Swedish Pirate Party which even gained access to the European Parliament, www.piratpartiet.se/international/english, last accessed on 30 August 2009.

[4] See Tal Z. Zarsky, *Law and Online Social Networks: Mapping the Challenges of User-Generated Information Flows, Fordham Intellectual Property*, 18 MEDIA AND ENTERTAINMENT LAW JOURNAL 741 (2008); Tal Z. Zarsky, *Thinking*

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

how far new network friendly rules might be conceived which not only do justice to the logic of the internet, but might reinforce it.

B. "Censorship in the internet"? The recent discussion on blocking access to sites containing child pornography

The new federal statute which gives the Federal Office of Criminal Investigation (BKA) the possibility to order internet service providers (ISP) to block access to sites containing child pornography[5] has raised a fierce controversy between the ruling political parties, in particular, and the internet community. Critics do not oppose the intentions of the legislator but the instruments used for their implementation into practice. This instrument is on one hand said to have little efficacy, but on the other hand is said to be a first step towards a comprehensive approach (some even go so far as to name it "Chinese") to control internet communication including political content.[6] This "slippery slope" argument deserves our interest not so much for the merits of its fight against censorship, but as a symptom of a youth culture – and of course adults which in general tend to regard youth culture as expressions of "freedom."

In this case a nomadic individualism[7] which regards any restriction of its choices as incompatible with the liberties guaranteed by the constitution. The concern for freedom of communication in the internet might appear understandable and even responsible. However, we have to accept that limits to civil liberties imposed by the legislator for behavior in the offline world with good reasons cannot be completely excluded from the internet, which is not exempt from criminality, harassment, mobbing, *etc*. It will be shown in this article that in fact the "balance of power" between freedom and control[8] is

---

Outside the Box: Considering Transparency, Anonymity and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society, 58 UNIVERSITY OF MIAMI LAW REVIEW 1301 (2004).

[5] For a description of the project see www.bmfsfj.de/bmfsfj/generator/BMFSFJ/kinder-und-jugend,did=126134.html, last accessed on August 30, 2009.

[6] Lutz Donnerhacke, *Die dreizehn Lügen der Zensursula* (19.4.2009), www.netzpolitik.org/2009/die-dreizehn-luegen-der-zensursula/, last accessed on August 30, 2009, - "zensursula" is the nickname for the Federal Minister *Ursula von der Leyen* who is responsible for this law ("zensur+ursula").

[7] For the overestimation of the creativity in the networks of the internet see ANDREW KEEN, THE CULT OF THE AMATEUR: HOW TODAY'S INTERNET IS KILLING OUR CULTURE (2007); GEERT LOVINK, ZERO COMMENTS. ELEMENTE EINER KRITISCHEN INTERNETTHEORIE (2008), in particular at 38; for a critique of the postmodern individuality see ANDREAS RECKWITZ, DAS HYBRIDE SUBJEKT. EINE THEORIE DER SUBJEKTKULTUREN VON DER BURGERLICHEN MODERNE ZUR POSTMODERNE, 532 (2006); CHARLES MELMAN, L'HOMME SANS GRAVITE 215 (2002).

[8] See Kim A. Taipale, *Data-Mining and Domestic Security. Connecting the Dots to Make Sense of Data*, 5 COLUMBIA SCIENCE AND TECHNOLOGY LAW JOURNAL 1 (2003); Kim A. Taipale, *Technology Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd*, 7 YALE JOURNAL OF LAW AND TECHNOLOGY 123, 190 (2004).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

disturbed in the internet because of the ease of access to and links between sites and addresses on the one hand and the reduction of the cost of communication on the other hand. This is valid for both communication and control. However, this problem cannot be solved by excluding any measure of blocking access to internet sites as a functional equivalent to confiscation in the offline-world.

In this case the consequences of anonymous communication in the internet would be borne entirely by those persons and institutions which are protected by the laws which impose limits on the use of freedom. The same would be valid in the reverse case; if one were to ignore the ease of electronic control over internet communication once introduced by general norms which do not pay attention to the specificity of the networks,[9] a new risk for freedom of communication would emerge. The confiscation of "real" media in the offline world is burdensome and visible to the public – this is an obstacle to efficient control which is favorable to the use of freedom. However, the dilemma cannot be ignored – though this is quite common in the internet community.

In my view this is a symptom of a lacking readiness to address the potential of a network-friendly type of law which might be prone to reducing the effects of this dilemma. Instead the freedom of the internet is understood as a kind of right to legal anarchy which in the internet seems to be completely inaccessible to any kind of restriction – at least efficient ones - which might well be acceptable in the offline world. This is incompatible with the principle of equal treatment of media content, not to mention the higher risk of internet transactions which might have detrimental effects on individual rights other than freedom of communication. The possibility of limiting access to illegal content is quite common in the offline world mainly for the protection of minors, – even without preceding judicial control (see further *Treaty of the Länder on Broadcasting and Treaty of the Länder on the Protection of Minors from Detrimental Media Use*). In the online world, apparently each and every intervention of the state into internet communication is regarded as disproportionate.

I. A case of censorship? Child pornography as opinion and information?

The ideological fixation on "censorship" tends to prevent a serious discussion on the question of whether or not pornography (explicit sexual material) has the characteristics of an "opinion" or of "information," which are protected by the liberties of communication, Art. 5 par. 1 of the Grundgesetz.[10] Which kind of opinion, and which type of information does the photograph of a child which has been degraded as a sexual object of adult

[9] Karl-Heinz Ladeur, *E-Bay-Bewertungssystem und staatlicher Rechtsschutz von Persönlichkeitsrechten*, 10 KOMMUNIKATION & RECHT 85 (2007).

[10] See generally HANS D. JARASS & BODO PIEROTH & BERNHARD SCHLINK, *Art. 5 No. 2*, in: GRUNDGESETZ, COMMENTARY (10th ed., 2009).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

contain? Though the possibility that a communicative value may be attributed to pornography cannot be ruled out,[11] this borderline type is apparently not at stake here. This is why, according to an interpretation which is discussed in the US,[12] the most widely spread versions of "explicit sexual" content is not protected by freedom of opinion or freedom of information at all: they do not communicate anything that might have an "intellectual effect" on the public or which seeks debate in the public fora. The dissenting opinion which comes to a different conclusion is mostly not given any argument. It seems to regard the inclusion of pornography in the protection of freedom of opinion as a given – which apparently it is not. As a consequence, blocking access to pornography in the narrow sense cannot be a case of censorship,[13] even if it is the object of control before being accessible to the public. The assumption that any blocking of access should be incompatible with the principle of proportionality is not plausible at all.

II. The generalized censorship of the internet ... is already here!

Even the reference to the risk of opening a new regime of internet control which is prone to be expanded to cover other content, including political communication, is not plausible. This is a typical "slippery slope" argument, which in this case misses the point completely because this "nightmare" has already come true – the internet community apparently not being aware of the internet law as it stands: § 59 pars. 2-4 RfStV[14] and § 20 par. 4 JMStV[15] give the competent authorities of the Länder the authorization to intervene in online media including the blocking of access to illegal content, and content that might harm the development of minors in particular. This possibility has already been made use of in a case concerning Nazi propaganda.[16] The author of this article has also criticized this authorization for formal reasons.[17]

---

[11] See *Reports of the Federal Constitutional Court* (BVerfGE) Vol. 83, 130 at 139.

[12] FREDERICK SCHAUER, FREE SPEECH: A PHILOSOPHICAL ENQUIRY 181 (1982).

[13] EKKEHART STEIN & GÖTZ FRANK, *§ 38 V* in: STAATRECHT (20th ed., 2007); WOLFGANG HOFFMANN-RIEM, *Art. 5 No. 93* in: ALTERNATIV-KOMMENTAR ZUM GRNDGESETZ (3rd ed. 2001); still relevant Helmut Ridder, *Das Zensurverbot,* 2 ARCHIV FÜR PRESSERECHT 882 (1969); the prohibition of censorship is by the way meant to protect the author of a communication, see only BODO PIEROTH & BERNHARD SCHLINK, STAATSRECHT II (21st ed. 2007), number 665.

[14] See only W. Schulz, *§ 59 No. 9* in: BECK'SCHER KOMMENTAR ZUM RUNDFUNKRECHT (Werner Hahn & Thomas Vesting eds., 2nd ed., 2008).

[15] Wolfgang Schulz & Thorsten Held, *id*., § 20 JMStV number 9.

[16] *Oberverwaltungsgericht* Münster, 56 NEUE JURISTISCHE WOCHENSCHRIFT 2183 (2003); a consenting commentary by Spindler & Volkmann, 6 MULTIMEDIA UND RECHT 354 (2003); see also EVA BILLMEIER, DIE DÜSSELDORFER SPERRVERFÜGUNG. EIN BEISPIEL FÜR VERFASSUNGS UND GEFAHRENABWEHRRECHTLICHE PROBLEME DER INHALTSREGULIERUNG IN DER INFORMATIONSGELLSCHAFT 163 (2007).

[17] Karl-Heinz Ladeur, *Der prozedurale Schutz der Medienfreiheit*, 48 Zeitschrift für Urheber- und Medienrecht 1 (2004).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

This measure has by far not raised a comparable public concern. Astonishingly, the general censorship infrastructure which exists already has not found the attention of the internet community. The recent discussion on the concrete measures against child pornography shows that there is no serious discussion on the structure of a net friendly internet law altogether.[18] The criticism is mainly driven by emotions whereas the existing law and potential alternatives are ignored. As a supplementary argument, it may be added that all the measures of censorship can be controlled by a judge. However, one need not be a prophet to predict that none of the measures will be brought to court.

C. Data protection in the internet – for a change from bureaucratic protection to net friendly proceduralization

I. From the protection of individual "ownership" of data toward the observation of data flows and nodes

The problems of data protection in the internet are so manifold that not all can be raised in the context of this article. This is also the reason why they cannot be tackled by clear-cut rules to be imposed on the net in advance, from outside. The steering of data-communication is impossible. This complexity can, however, be tackled by a version of proceduralization of the legal order of the self-organization process which the internet undergoes as the network of networks. The internal differentiation of the legal structure of the internet may allow for the generation of new knowledge and its processing via specific institutions of the internet.

A net-specific problématique of the implementation of legal controls consists in the discrepancy between the attention which the single data of the individual meets on the one hand, and the values of the processing and relationing of data through data mining, the construction of personality profiles[19], the observation of broad data flows, and the operation of linking data by firms and by the state for reasons of security. The interest in closure and disclosure of information are both legitimate.

II. The necessity to observe the collective effects of the processing of data flows

[18] There are some exceptions which should be mentioned CHRISTOPH FIEDLER, MEINUNGSFREIHEIT IN EINER VERNETZTEN WELT (2002); see also *id*., DIE FORMALE SEITE DER ÄUSSERUNGSFREIHEIT. ZENSURFREIHEIT UND ÄUSSERUNGSGRUNDRECHTE (1999); VAGIAS KARAVAS, DIGITALE GRUNDRECHTE: ELEMENTE EINER VERFASSUNG DES INFORMATIONSFLUSSES IM INTERNET (2007).

[19] See JOSEPH TUROW & LOKMAN TSUI, THE HYPERLINKED SOCIETY: QUESTIONING CONNECTIONS IN THE DIGITAL AGE (2008); Karl-Heinz Ladeur, *Datenverarbeitung und Datenschutz bei neuartigen Programmführern in "Virtuellen Videotheke*n," 3 MULTIMEDIA UND RECHT 715 (2000).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

It would be much more helpful to change the paradigm of the conception of data protection 2.0 to a focus on networks, *i.e.* to have a closer look at the opportunities and risks of data processing in networks and to adapt its legal structure which is still characterized by its origin in the offline world to the conditions of the media world.[20] The rapid proliferation and continuous linking of information in networks can no longer be adequately mirrored in the individual right to decide on separate domains of action which are attributed to persons. This construction can no longer do justice to the hybridization of legal constellations. For example: a firm can possibly generate a high information value by data-mining,[21] which does not correspond to the construction of an accumulation of infringement of individual rights to decide on the use of the data which are of no particular interest to the user himself. A hybrid construction which is more adapted to the collective trans-subjective component of the data in a network can bring a more flexible and adequate solution to this dilemma (see below).

A case for a reconceptualization of data protection is the deanonymization of IP-addresses by private persons or the public security agencies. In this respect it should be taken into consideration that the internet as the network of networks cannot be dissolved into a number of linear relationships of exchange between individuals - the precondition of the older regime of protection of protection of privacy in telecommunications - but that the old telecommunication has been transformed into an online world with its own rationality of information processing und generation of new information products which is based on the generation of collective and collateral effects between information. These trans-subjective effects can no longer be attributed to individual "owners." Examples of these new phenomena are eBay ratings[22] and ratings of professional achievements (teachers, professors, medical doctors *etc*.).[23]

[20] For a first attempt to give an overview of the problems of privacy in the "social media" see James Grimmelmann, *Facebook and the Social Dynamics of Privacy*, 94 IOWA L. REV. 4 (2009).

[21] BING LIU, WEB DATA-MINING: EXPLORING HYPERLINKS, CONTENTS AND USAGE DATA (2007).

[22] In the US eBay offers an electronic mediation procedure via "Square Trade;" www.ebay.com/services/buyandsell/disputeres.html, last accessed on August 30, 2009.

[23] Karl-Heinz Ladeur, *Die Zulässigkeit von Lehrerbewertungen im Internet,* 56 RECHT DER JUGEND UND DES BILDUNGSWESENS 16 (2008); the Federal Court of Justice (*Bundesgerichtshof*) has regarded ratings of teachers as legal, see Dec. of June 23, 2009, VI ZR 196/08; for cyber-mobbing in schools in the US see Rita J. Verga, *Policing their Space: The First Amendment Parameters of School Discipline of Student Cyberspeech*, 23 SANTA CLARA COMPUTER AND HIGH TECHNOLOGY LAW JOURNAL 727 (2007); with respect to the differentiation of different types of public spaces in the internet era see JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT 213 (2009), where classrooms e.g. are regarded as "private public spaces" which should not be turned into "public public spaces"; otherwise there would be a pressure to be always on "press conference behavior".

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

The ubiquitous nature of the internet and its new logic comes also to the fore when we take a look at the transformation of the relationship between different types of rights which have been developed and coordinated in the offline world and migrate into the internet. It is inevitable that this entails a major effect of destabilization which has to be compensated by a rebalancing. A major part of the internet community does not accept that the unbalanced relationship between the protection of intellectual property and "fair use"[24] which has come about in the process of digitalization of information needs rebalancing. One has to bear in mind that in the offline world the number of copies made from a CD is limited by the cost of distribution; illegal public use of protected content can be observed with a certain investment of time and money. The rise of new technologies has already in the past been an issue which has led to some rearrangement of intellectual property and its limits. However, in the online world the ease of proliferation of protected content via hybrid ways of transfer and exchange among unknown persons (peer-to-peer) has delimited any understanding of fair use. A compensation of this process of undermining the hitherto established "informational division of powers" would only be possible by search processes on the side of the bearers of rights in digital forms, as well. This is regarded as an infringement of the right to privacy in the internet community, though this only compensates for the hybridization of massive distribution processes among individuals who do not know each other. It should be accepted that this unbalancing, which is brought about by the architecture of the internet, needs a certain recompensation by a re-entry of a new type of action for the protection of intellectual property into the domain of options of the internet. Otherwise the balance would be completely disturbed.[25]

Something similar could be said for security issues: in the offline world the state has a lot of formal and informal instruments of observation and investigation in criminal procedure. Traces can be analyzed, testimonials can be collected, experts can be asked, *etc*. In the internet, "traces" are always digitized; they can only be analyzed if this possibility is introduced into the architecture of the net. If one were to leave this disruption aside, data protection would end up as systematic protection of criminal wrongdoers. In the offline world, protection of privacy, the secrecy of telecommunication, and the presumption of innocence in particular abuse, and the possibility of "false negatives" in criminal investigation is accepted because otherwise unintended perverse effects might have a repercussion on freedom in general and generate a chilling effect on communication by

[24] For a European perspective see P. Bernt Hugenholtz, *Copyright and Freedom of Expression in Europe*, in EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY, 343, 352. (Rochelle Cooper Dreyfuss, Diane Leenheer Zimmermann & Harry First, eds., , 2001).

[25] See Karl-Heinz Ladeur, *Der Auskunftsanspruch der Rechteinhaber nach § 101 n. F. UrhG und der Datenschutz – Geht der Anspruch mangels Daten ins Leere?*, 105 URHEBER-, FILM- UND THEATERRECHT UFITA 443 (2009).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

telephone.[26] If, however, the collection of proofs meets a systematic difficulty linked to the whole technological structure of the online world, this would again change the balance between the rights and public goods which are at stake in this constellation. It would generate the certainty that one could not be prosecuted for criminal acts committed under the protection of anonymity in the online world.

The "chilling effect" would in this case be created on the side of the potential victims of criminal acts and the state. This is why anonymity cannot be given such far reaching protection against criminal investigation. On the other hand, one has to admit that the reverse reaction – the unlimited expansion of public privileges for investigation in criminal procedure - would create a new imbalance because it would ease the investigation even below the threshold of risks which can be attributed to concrete action. On the other hand, one has also to consider that the flexible internet communication simplifies the preparation of serious criminality by the protection of anonymity. And in addition to this one has to bear in mind that the limited intrusion into the preparation of criminal acts is not without preconditions: it is based on the assumption that – in political criminality in particular – the plans to commit, for example, a terroristic act may be hampered by the influence of the public fora (discussions with others, radio, TV, press *etc*.).[27] On the other hand, the internet brings to the fore a whole range of new networks which are completely closed off from any irritating influence from other groups, ideas, *etc*. The internet is a network of networks, but this does not mean that all the networks are interrelated; on the contrary.

III. The self-organization of the "data-owners" following the example of"„collecting societies" in the protection of intellectual property: An example for a net friendly legal instrument

A new "control regime"[28] which is fine tuned to the functioning of the internet and the processing of data and patterns of combination could, for example, consist in the public and private funding of self organized private institutions for the protection of data in the internet following the model of collecting societies in intellectual property law and practice.[29] Such a new type of association of users might act as (information broker in the

[26] For communication in general see Frans Birrer, *Data Mining to combat Terrorism and the Roots of Privacy Concerns*, 7 ETHICS AND INFORMATION TECHNOLOGY 211 (2005).

[27] See the overview in MARK A. GRABER, TRANSFORMING FREE SPEECH: THE AMBIGUOS LEGACY OF CIVIL LIBERTARIANISM 144 (1991).

[28] HARRISON C. WHITE, IDENTITY AND CONTROL, HOW SOCIAL TRANSFORMATIONS EMERGE 345 (2nd ed., 2008).

[29] Karl-Heinz Ladeur, *Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken,* 24 DATENSCHULTZ UND DATENSICHERHEIT 12 (2000); for a critique to "economize" data following the model of intellectual property rights, see Thilo Weichert, *Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung*, 54 NEUE JURISTISCHE WOCHENSCHRIFT 1463 (2001).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

sense of a representation of the hybrid public-private interests of the users which transcend their own limited privacy concerns and are focused on the trans-subjective elements of data processing in the Internet. These associations could make contracts on the conditions of the use of data that are not of much concern for each individual. This approach could correspond to the new trans-border effect, which is common for the internet use of data inasmuch as it raises collective effects from mass transactions which hitherto did not have any relation except to a central agent (such as a broadcaster). This information broker might make contracts on payment for the use of internet data or make contracts on the quality of protection of privacy. This form might be a productive alternative to the bureaucratic form of data protection by the institution of a public officer for the protection of privacy (*Datenschutzbeauftragter*).[30] This model could present the appropriate levels of flexibility and hybridization (balancing individual and collective interests) which are required by the logic of the internet, whereas traditional legal instruments and procedure are more based on the expectation of stability of rights and public goods.

A new control regime has to adapt to the volatility and ubiquity of internet communication by flexible self-organization of legal positions which are involved in a procedural mode of permanent self-transformation. It has to react to the fact that even identities are no longer stable but are "sampled" and open to transformation.

D. Improving the protection of intellectual property in the internet by communication with "avatars"

I. Communicating with pseudonyms

The protection of intellectual property in the internet meets a host of difficulties worldwide.[31] The German legislature has created a right to information of right holders against internet service providers (ISPs) in the case of digital downloads which have been detected by the identification of the IP-address (which can only be de-anonymized by the ISP itself).

[30] Obviously there are limits to the individual decision on data but this process of self-organization might also help determine these limits.

[31] See Ladeur, *id*. (UFITA...); for the UK see "Court rules against song swappers", BBC NEWS, 27 January 2006; for the US "Millionenstrafe im US-Filesharer-Prozess," Heise-Online, 19 June 2009; for a new model of a flexible management of copyright see Bennett M. Lincoff, *A Plan for the Future of Music Performance Rights Organizations in the Digital Age*: (Dreyfus *et al*., eds., *id*.) 167.

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

The problems which are raised by this conflict cannot be analyzed in detail in this article.[32] Only the fundamental challenge of technology-induced change of the division of power between the rights which are at stake here shall be highlighted.

A flexible solution to the problem of the mass of potential conflicts and the necessity to decide on the de-anonymization by a judge (§ 101 par. 9 Intellectual Property Law/*Urheberrechtsgesetz*) could consist in the creation of a "clearing house"[33] which could organize a procedure for the warning of offenders via email (without de-anonymization). This clearing house could be composed of representatives of the right holders, the ISPs and a data protection officer. It could also formulate standards and rules for its procedure and implement the right to be heard for the offender.

The issue of data protection[34] would be satisfied by the provision that the identity of the offender and the details of the offense would be "frozen" in a "hash value"[35] – a code consisting of numbers which alone would be accessible to the clearing house, whereas the key which would allow for de-anonymization would be excluded from the right holders.[36] This hash value would constitute at the same time a kind of avatar, the use of which would allow for the offender to communicate by email with the body under a pseudonym.

It would be imaginable to introduce as a second instance a kind of self-organized "cyber court"[37] composed of independent lawyers who would again communicate with the offender by his avatar.[38] The basis of this procedure could be integrated in the conditions

---

[32] Ladeur, *id*. (UFITA).

[33] Karl-Heinz Ladeur, *Die gemeinsame Clearing-Stelle von Rechteinhabern und Providern,* 11 KOMMUNIKATION UND RECHT 695 (2008) (the article is based on expertise of the German music and film industry).

[34] See Gerald Spindler, *Der Auskunftsanspruch gegen Verletzer und Dritte nach § 101 UrhG,* 52 ZEITSCHRIFT FÜR URHEBER- UND MEDIENRECHT 640 (2008).

[35] www.itwissen.info/definition/lexikon/hashwert.hash-value.html

[36] Not differentiating sufficiently: Franziska Raabe, *Urheberschutz im Internet und seine Einfügung in den Gesamtrechtsrahmen*, 50 ZEITSCHRIFT FÜR URHEBER- UND MEDIENRECHT ZUM 439, 442 (2006); the *Bundesrat* (the representation of the *Länder*) has taken a different position with respect to the necessity to make information on the identity of downloaders dependent on the decision of a judge, BT-Drs 16/5048, 53ff. 56f.

[37] See Lucille M. Ponte, *The Michigan Cyber Court: A Bold Experiment in the Development of the First Online Courthouse,* 4 NORTH CAROLINA JOURNAL OF LAW AND TECHNOLOGY 51 (2002) for state courts. The article refers to private self-organized cyber courts which would establish their own network-based rules which can adapt more easily to the necessity to bear in mind the law making function of communication networks in the internet, see Yannick Gabuthy, Bruno Deffains & Philippe Fenoglio, *An Economic Analysis of Conflicts Resolution in Cyberspace*, in INTERNET AND DIGITAL ECONOMICS, 539, 542 (Nicolas Curien & Eric Brousseau, eds., 2007).

[38] For a theoretical approach to electronic agents and their legal status, see Gunther Teubner, *Elektronische Agenten und Grosse Menschenaffen – Zur Ausweitung des Akteursstatus in Recht und Politik* 27 ZEITSCHRIFT FÜR RECHTZIOLOGIE 5 (2006).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

of use formulated by the ISP. A law would not be necessary because the warning would be nothing but a measure for the implementation of the contract and for the prevention of abuse.[39] The new information right can be regarded at the same time as the legal basis for the collection of the transaction data.

II. Alternative: Private-public co-regulation based on a law

An alternative to a purely contractual solution (contract right holders and ISP and ISP/user) could be seen in a law which would force ISPs to set up a warning regime by themselves, and at the same time allow them to meet this requirement by a cooperative procedure following the model described above. It could at the same time impose documentation requirements which would at the end of period of experimentation allow for an evaluation. This model has the advantage that it does not use the kind of controversial sanction of exclusion from the use of the internet for a limited period which a French law had chosen (*Loi Olivennes*).[40] The French Constitutional Council[41] has in the meantime declared this part of the law to be unconstitutional because of the far reaching effect on the freedom of communication and information. The model proposed here differs from this solution as well with respect to legal basis of the warning procedure; he French Model has foreseen the creation of a new state agency (HADOPI), whereas here a contractual model based on private law is given preference.

E. Criminal law and criminal procedure in the face of "risky networks"

I. From organized criminality toward "criminal networks" – the example of Al Qaeda

On February 27th, 2008, the German Federal Constitutional Court[42] pronounced a new fundamental decision on online investigation for the purpose of criminal prevention. It has pronounced a new "computer freedom"[43] in the sense of the protection of confidentiality and integrity in electronic systems as a new version of the protection of privacy. One may doubt that this general construction fits the emerging logic of networks because the internet is not just a means communication but of production of informational goods and

[39] Ladeur, *id.* (UFITA...).

[40] See www.numerama.com/magazine/8657, last accessed on 30 August 2009.

[41] Conseil Constitutionnel 2009-580 DC, 10 June 2009, www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-décisions/2009/decisions-par-date/2009/2009-580-dc/decision-du-10-juin-2009/42666/html

[42] Federal Constitutional Court (*Bundesverfassungsgericht*), 61 NEUE JURISTICHE WOCHENSCHRIFT 822 (2008).

[43] See the comment by Martin Eifert, *Informationelle Selbstbestimmung im Internet*, 28 NEUE ZEITSCHRIFT FÜR VERWALTUNGSRECHT 521 (2008).

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

bads as well. From the point of view of the public authorities a balance has to be struck between the protection of informational actors and networks on one hand, and on the protection from the perverse effects of the confidentiality[44] of the internet in particular. The internet is not a more sophisticated version of the telephone, which is a means of individual exchange. It is a whole new online world, a network of networks, including a whole range of different formats and regimes which cannot be paralleled with anything we have known in the past. For example: the *Bundesverfassungsgericht* (Federal Constitutional Court) has already in the past reduced the level of protection for conventional telecommunication, which abuses the anonymity of electronic contacts for criminal purposes or for anonymous harassment. [45] This looks obvious: why should a person deserve the procedural aspects of the protection of telecommunications for direct criminal purposes? (This is not to be confounded with the control of the *content* of communication.)

In the internet one has to be aware of the fact that networking as such can be an efficient form of preparing and committing criminal acts which would not be imaginable in traditional telecommunication. So, why should all parts of the network of networks deserve the same level of protection? This cannot be a consequence of the new computer freedom.

The court formulates a number of requirements for online investigation[46] for purposes of public security in particular, *i e.* the concrete threat of a danger to be expected for an important public good on the basis of concrete facts which in general have to be checked by a judge. One has to bear in mind that a new type of criminality is emerging, what I would call "network criminality." In the field of terrorism, no longer primarily concrete acts are to be feared which can be attributed to persons. At the same time risky networks come to the fore which can no longer be regarded as mere preparatory communications that from a legal point of view are irrelevant below a concrete step of implementation of a criminal plan. The inherent risks of such criminal networks have to be reduced to a certain extent in a strategic mode, their "costs" have to be raised once a clear-cut prevention of any criminal action would appear to be an illusion. Terroristic activities of Al Qaeda[47] and like networks are processed in postmodern fractal "cellular businesses" in which different ideological, military, informational, financial, communicative, *etc*., operations are aggregated in a heterarchical "virtual organization." Criminal law had to adapt to the emergence of organized criminality (*e.g.* by the adapting doctrine to collaborative action),

[44] See for the English conception of privacy as a regime of "confidentiality" Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEORGETOWN LAW JOURNAL 123 (2007) 123.

[45] Federal Constitutional Court (*Bundesverfassungsgericht*), BVerfGE 85, 386.

[46] Federal Constitutional Court (*Bundesverfassungsgericht*), 81 NEUE JURISTICHE WOCHENSCHRIFT 822 (2008).

[47] See RAND Document *"Beyond Al-Qeida,"* 2 Vols., 2006.

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

and the same will be inevitable for "criminal networks." The forms of criminality follow the transformation of the legal evolution of cooperation; in the network society[48] we have networked criminality.

As in franchising networks,[49] we find central integrative nodes (for the ideology). Apart from this element we have "strings" which are set up for the collection of data, the financial transactions which on the face appear to be harmless and do not allow for the identification of "concrete facts" which can be read as the starting point of a criminal act. The functioning of the "risky networks" could not be observed at all if any investigation could only be focused on concrete "facts." Liberal institutions are adapted to handle danger which can be attributed to persons. They have difficulties in addressing the risk related to criminal organizations, but they have yet to meet the challenge of risky networks.

II. Criminal procedural investigation

Individuals move actively through the internet with the use of a pseudonym as a kind of avatar. The same could be imagined in the reverse role when they are partially identified as nodes in a risky network: in order to limit public collection of data one can choose an objective limit and reduce investigation by formulating a high level of intervention ("concrete facts").[50] One could also think about a subjective mode of limiting the linkage of the data found in the internet to the real name of a suspicious person in the offline world. To a certain extent only this avatar of a person may be constructed and used as a frame of reference for the collection of data. Only a second level of investigation would allow a link between the online and offline worlds.[51]

The technical basis of such a differentiation could again be seen in the possibility of calculating a hash value which freezes the data and the potential IP-address or other ways of access to the real world in a numerical code and deposits the key to the offline world at a separate institution which might be organized as a kind of cyber court within the agency. The technique of erecting firewalls within the net which separate different informational regimes could be transferred to public investigation procedures. Control regimes could be differentiated according to the potential of the internet and its relational rationality.

[48] MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY, VOL. 1: ECONOMY, SOCIETY AND CULTURE (2000).

[49] GUNTHER TEUBNER, NETZWERK ALS VERTRAGSVERBUND: VIRTUELLE UNTERNEHMEN, FRANCHISING, JUST-IN-TIME IN SOZIALWISSENSCHAFTLICHER UND JURISTISCHER SICHT 215 (2004).

[50] Federal Constitutional Court (*Bundesverfassungsgericht*), 81 Neue JURISTICHE WOCHENSCHRIFT 822 (2008).

[51] Taipale, *id*.

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press

A major part of the public concerns about the increasing data collection in public agencies could be mitigated with such a net friendly strategy. At the same time such a formalized operation with firewalls within state bureaucracy might allow for better control than an unstructured mass of data which is collected and processed according to different patterns and rules. The strategy of public officers of data protection to declare any data to be sensitive in advance is not adapted to the strategic mode of operation in networks.

Data protection and its control regimes in the internet have to be conceived in a net-related mode. They should focus on nodes of relationships in networks and not (primarily) on persons. (Obviously there are types of data which are sensitive from the outset, *e.g.* data on health, but this is not the rule.)

F. Outlook

We need "traffic rules" for the internet and the information society, not the protection of any data of a nomadic individualism which fights against any restriction of its autonomy. A network friendly internet law could make use of the technological flexibility of a digital relational rationality. Data protection is not the core element of civil liberties as its protagonists sometimes try to make the public believe. The risks of the new technologies and the potential perverse side effects of its use can only be managed within the domain of options which the digital online world has created. Hybridization and the proliferation of linkages through networks are two of the characteristics of the internet. Instruments for the protection of the variety of the internet and the limitation of state power in the network of networks should make use of these paradigmatic phenomena.

https://doi.org/10.1017/S2071832200018101 Published online by Cambridge University Press