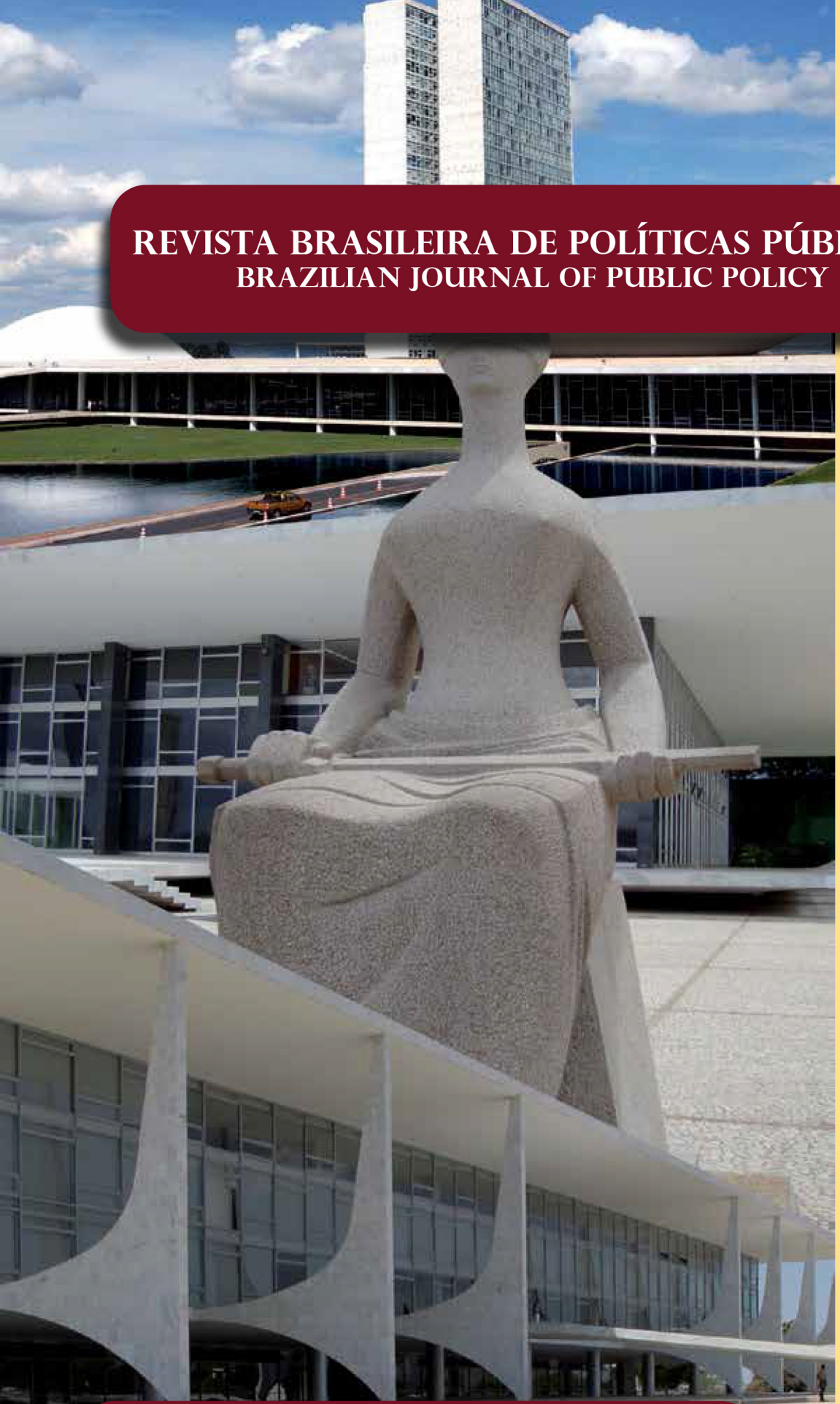

UniCEUB
ISSN 2236-1677

REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS
BRAZILIAN JOURNAL OF PUBLIC POLICY

New institutions for the protection of privacy and personal dignity in internet communication – "information broker", "private cyber courts" and network of contracts

Novos Institutos para a Proteção da Privacidade e Dignidade Pessoal na Comunicação pela Internet - "Corretor de Informaçôes", "Cortes Privadas Cibernéticas" e Redes de Contratos

Karl-Heinz Ladeur

VOLUME 3 • N. 2 •JUL - DEZ 2013

Sumário

Dossier Federalismo

Artigos sobre outros temas

doi: 10.5102/rbpp.v3i2.2531

New institutions for the protection of privacy and personal dignity in internet communication – "information broker", "private cyber courts" and network of contracts

Novos Institutos para a Proteção da Privacidade e Dignidade Pessoal na Comunicação pela Internet - "Corretor de Informaçôes", "Cortes Privadas Cibernéticas" e Redes de Contratos

Karl-Heinz Ladeur**

Abstract

Symposium "Beyond Montesquieu: Re-thinking the architecture of contemporary governance": The internet needs new types of legal ordering, which are adapted to self-regulation and the rapid transformation of knowledge and social norms. Data protection, public investigation, "social media" and financial markets challenge the classical orientation of the legal system towards individual behaviour. The new "addressees" of law are networks as quasi-subjects. New regimes of proceduralisation can structure the development of a "net-friendly" paradigm of a law beyond the individual. The article tries to demonstrate the feasibility of such a model with reference to the above-mentioned challenges.

Keywords: Privacy, Internet, Private Courts, Networks

Resumo

A internet precisa de novos modelos de regulação jurídica, adaptados para a auto-regulação da rápida transformação do conhecimento e das normas sociais. A proteção dos dados, a pesquisa pública, a "mídia social" e os mercados financeiros desafiam a orientação clássica do sistema jurídico para a regulação dos comportamentos individuais. Os novos "destinatários" do direito são as redes que figuram como quase-sujeitos. Os novos regimes de procedimentalização pode estruturar o desenvolvimento de um paradigma jurídico "net-friendly" para além do indivíduo. O artigo procura demonstrar a viabilidade de um tal modelo com referência aos desafios acima mencionados.

Palavras-chaves: Privacidade, Internet, Mecanismos Privados de Solução de Conflitos, Redes

* Recebido em 11/08/2013
Aprovado em 21/08/2013

** 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. 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" (Elie Noam)[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, both concerning the traditional conflict of "the man versus the state" and the new constitutional dimension of legal conflict between private persons (and organizations), it shall be tested how far new network friendly rules might be conceived which not only do justice to the logic of the internet, but might reinforce it.

2. Protection from offensive communication in the internet (blogs etc.)

2.1. The structure of media law and the transformation of social norms as its infrastructure

The reciprocal adjustment of the private and public domains, and, as a consequence, the limits of the distribution of knowledge (and ignorance/secrecy), in the past, followed a kind of "separation of powers" inherent in the knowledge basis of society.[5] These "knowledge rules" cannot be reduced to simple and static border concepts, but were founded on a complex infrastructure of a plurality of legal and social norms, which included bridging concepts and meta-rules on the conflict of norms – both explicit and implicit.[6]

On the one hand, a media-related law of libel and slander about the limits of public communication has evolved over a long period of time. On the other hand, it should not be overlooked that, at the same time, the oral medium of "rumour" allowed for types of communication that remained beyond the control of the law – and not just under conditions of tight social control of communication.[7] However, a multiplicity of stop rules of discretion, of separations between the private and the professional, the private and the political, the spatial limits of the expansion of "rumours", the differentiation of different *fora* (art and newspapers, for example), as well as rules of hypocrisy (paying lip-service to the recognition of "honour" in public while, at the same time, secretly spreading unpleasant

1 See Yochai Benkler, The Wealth of Networks (Yale UP, 2006); Clay Shirky, Here Comes Everybody: The Power of Organizing without Organization (Penguin Books 2009); Lawrence Lessig, Code and Other Laws of Cyberspace (Basic Books 2006), who describe the new logic of the internet as not only a new means of communication.

2 Interconnecting the Network of Networks (MIT Press 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; the German Pirate Party has in the meantime even become more successful.

4 See Tal Z. Zarsky, *Law and Online Social Networks: Mapping the Challenges of User-Generated Information Flows*, 18 Fordham Intellectual Property, Media and Entertainment Law Journal 741 (2008); Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity and Pseudonimity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 University of Miami Law Review 1301 (2004).

5 See Geoffrey R. Stone, *Privacy, the First Amendment, and the Internet*, in: Saul Levmore & Martha C. Nussbaum (eds), The Offensive Internet. Speech, Privacy, and Reputation, (Harvard University Press, 2010), 174, at 180.

6 See Karl-Heinz Ladeur, *Helmut Ridders Konzeption der Meinungs- und Pressefreiheit in der Demokratie*, 32 Kritische Justiz, 281 (1999).

7 Cf. Lior J. Strahilevitz, *A Social Networks Theory of Privacy*, 72 University of Chicago Law Review, 919 (2005).

or spiteful gossip) and the respect for the protection of "appearances" as a cultural achievement (as opposed to claims of "essence" and truth) have contributed to the emergence of a complex architecture of overlapping rules of co- and sub-ordination, specification of situations that have transformed the private as much as the public into a multi-faceted construction that has been processed by different social institutions.[8]

All in all, one can start from the assumption that the historical processes of change are related to the evolution of a paradox, the production and protection of the "individual of society" (Markus Schroer), whose form by itself is related to the different regimes of individuality and its normativity. As a consequence, the construction of "privacy" and its complex rules and patterns is also based upon the idea of a reproduction of society and not upon the right of the individual "to be let alone".[9] The observation and evaluation of "private" behaviour in well-defined spaces and integrated communities were both based upon the protection and the continuation of social norms.[10]

The same is true for the construction of "publicity", which produces forms of differentiation and specification with respect to the development of social memory, the processing of common themes for social communication, different *fora* of exchange (the media), the private-public spheres of the formation of individuals (family, church, school, reading of canonical texts) and the state as the centre of public decision-making.[11]

2.2 The great unbundling" of the media and its impact on social norms

One of the crucial phenomena of the transformation of the media and their public in postmodernity is to be seen in a tendency towards "the great unbundling", a formulation which the American Federal Communications Commission (FCC) has chosen for the description of the tendency towards more specialisation and the decline of a focused public of common interests which had been centred around the state in the past.[12] This evolution finds its repercussion in an increasing tendency to de-contextualise freedom of opinion and to transform it into a right to unlimited self-expression devoid of any public requirements or borders: the American Civil Liberties Union (ACLU) tends to combat any restriction of freedom of opinion as being prone to the creation of "chilling effects" in the individual: in cases of "cyber-mobbing", for example, the ACLU tends to act as *amicus curiae* with the clear intent to protect any communication, even the most degrading depiction of teachers in the internet (teachers being shown as decapitated on electronically manipulated photos or other images), whereas the protection of competing interests is regarded as the competency of "pedagogical measures".[13] This is characteristic of the new evolution towards a blurring of the limits and distinctions that had been the object of the above-mentioned architecture of norms on the inter-relationship between the public and the private in the past, and is now regarded as a "right to be let alone" or to communicate with "friends" without being bothered by any unintended third-party effect.[14] Whereas, in modernity, the "chilling effect" was invoked as a risk to the *public* function of freedom of opinion, the blurring of borders between the private and the public is characteristic of the hybridity of the new media.[15]

8 See generally Karl-Heinz Ladeur, Das Medienrecht und die Ökonomie der Aufmerksamkeit (von Halem: 2007).

9 Privacy has paradoxically always had different social dimensions, Levmore & Nussbaum, *Introduction*, in: *idem* (eds), *supra* note 5, 1, at 10.

10 Strahilevitz, *supra* note 7; Diane L. Zimmermann, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 Cornell Law Review, 291, at 332-334 (1983).

11 Cf. for the state-centred conception of publicity Federal Constitutional Court, Reports (BVerfGE) Vol. 7, 198 at 208; vol. 5, 85 at 205.

12 Federal Communications Commission (FCC), "The Changing Media Landscape in a Broadband Age", (June 2011), available at: www.fcc.gov/infoneedsreport.

13 Cf. Karl-Heinz Ladeur, *Rechtsfragen des „Cyberbullying" an Schulen und der Lehrerbewertungsportale in den USA, Frankreich und Deutschland*, 7 Recht und Bildung, 3 (2010/1).

14 Cf. the timely theoretical reconstruction of the role of freedom of opinion in a liberal society and the rationale of its limits John Deigh, "Foul Language: Some Ruminations on Cohen v. California", in: Levmore & Nussbaum, *supra* note 5, 195, at 210-212.

15 Anyone who has doubts about the necessity to impose limits on offensive internet speech should read the impressive article by Brian Leiter, *Cleaning Cyber-Cesspools: Google and Free Speech*, in: Levmore & Nussbaum, *supra* note 5, 155, at 168, which combines case analysis and insightful theoretical reflection.

This shift demonstrates the legitimacy of a retrospective on the normative and social *rules* that have determined the acceptability and attunement or evolution of themes in the "old media" (including oral gossip) in explicit legal and implicit social forms: one of the aspects of this normative definition of limits or relevance could be seen in the preservation of social trust in the professional standards of journalism that should be developed by the media as a kind of "epistemic rules", and which served as a frame of reference in the process of the definition of the legal borders of public and private communication. The obligation to control the truth of a factual claim communicated through the media, the separation of comment and message, reflection on the difference between the private and the public, *etc.*, are the foundations of a process of the self-stabilisation of a set of professional rules by which the media have to abide and whose generalisation allows for the development of a reliable legal standard of control. The professionalisation of journalism and the centralisation of the "epistemic rules" that courts have to draw upon allows for a stable practice of differentiation between knowledge and ignorance, the distribution of communications and secrecy.

Apparently, this complex architecture of norms is severed by the anarchic and heterarchic character of Internet communication.[16] Do we need new "net friendly" institutions for the protection of the personality rights or the secrecy and ignorance that could conflict with general assumptions about the "freedom of internet"?[17]

It could be imaginable to respond to the hybrid character of the new media and the tendency to blur the separation of the public and the private by a legal model that corresponds to this hybridity and which would start from the idea, first of all, of observing the societal basis for the self-organisation of the new rules for communication in conditions of complexity, and to use the legal system, court practice in particular, as a reflexive layer of normative re-coding in the mode of a "regulatory agency". In the next paragraph, a further example for a new regulatory function of private law and private law courts will be given. The dynamic transformation of both social and legal norms has an impact on the function of courts, as private actors tend to transform the stable foundations of a spontaneously-evolving common experience. This can be demonstrated with a view to transnational private law in general, and the ICANN-rules in particular.[18] As a consequence, one could think, as a first step, of imposing a new responsibility for the management of the rules of Internet communication on the providers. This could be done by a combination of "the carrot and the stick": limits imposed on the liability of providers for third-party communication could be made dependent on the establishment of private institutions of an alternative dispute-resolution procedure that would allow for a preliminary settlement of a conflict about conflicts between freedom of opinion and the protection of personality rights. A kind of private, albeit neutral, "Cyber Court" could act as an arbitrating body[19] which establishes a cheap and simple mode of decision-making upon the basis of a few flexible procedural rules (only by electronic communication).[20] One could even think about enabling participation by an "avatar" or the email address. All users of Internet services could be obliged to accept such arbitration provisionally, although this should not exclude the possibility of bringing these cases to ordinary state courts. All privileges of restricted liability, etc., could be formulated under the condition that the provider has to establish a functioning mode of arbitration. State courts would, in this case, act as a kind of second instance courts with the function of controlling the private self-regulation[21] as it is managed by the "cyber courts".

16 See, for the "imbalance" between privacy and freedom of opinion, Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, in: Levmore & Nussbaum, *supra* note 5, 15, at 27.

17 See for the US the discussion on anonymous advertising in the (for example apartments for: "whites only"), Rachel M. Kurth, *Striking a Balance Between Protecting Civil Rights and Freedom of Opinion*, 26 Cardozo Arts & Entertainment Law Journal, 805 at 832 (2008).

18 For the evolution of a transnational law beyond the state in general, see Oren Perez, *Normative Creativity and Global Legal Pluralism: Reflections on the Democratic Critique of Transnational Law*, 10 Indiana Journal of Global Legal Studies (2003) available at: http://www.repository.law.indiana.edu/ijgls/vol10/iss2/2.

19 See for the US Olivera Medanica & Kaiser Wahab, *Social Media, Recent Developments and Legal Considerations*, 26 Cardozo Art & Entertainment Law Journal, 237, 266 *et seq.* (2008), who propose a "notice and take down"-rule for libel incombination with a requirement to take the case to court within 10 days. In addition to this they favour the creation of an insurance fund for the compensation of harm inflicted on persons via the internet.

20 See, for a similar approach, Leiter, *supra* note 15, at 170, for search engines like Google.

21 Cf. only Gralf-Peter Calliess & Peer Zumbansen, Rough Consensus and Running Code – A Theory of Transnational Private

Both levels of "private law regulation"[22] could be expected to observe and evaluate primarily patterns of communication, to block problematical forms of communication or to strengthen productive models, new procedures, and, in the long run, the emergence of new rules that would correspond to the old architecture of social and legal norms on social communication and the relationship between knowledge and ignorance. Those providers who failed to act in conformity with these requirements would be treated as if they followed only private interests (and would not support a public system of communication).

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

3.1 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[23], 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.

3.2 The necessity to observe the collective effects of the processing of data flows

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.[24] 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,[25] 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 transsubjective 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 both private persons and the public security agencies. In this respect it should be taken into consideration that the internet

Law (Hart Publishing 2010, at 134-152.

22 For a theory of regulation, see Julia Black, *Proceduralising Regulation*, Parts I and II, (2000-2001) 20-21 Oxford Journal of Legal Studies, 597 (2000) & , 33 (2001).

23 See Joseph Turow & Lokman Tsui, The Hyperlinked Society: Questioning Connections in the Digital Age (University of Michigan UP, 2008); Karl-Heinz Ladeur, *Datenverarbeitung und Datenschutz bei neuartigen Programmführern in 'Virtuellen Videotheken'*, 3 Multimedia und Recht 715 (2000).

24 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 Law Review 1137 (2009).

25 Bing Liu, Web Data-Mining: Exploring Hyperlinks, Contents and Data Usage (Springer, 2007).

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 transsubjective effects can no longer be attributed to individual "owners." Examples of these new phenomena are eBay ratings[26] and ratings of professional achievements (teachers, professors, medical doctors *etc.*).[27] 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.

3.3 The self-organization of the "data-owners"vis-à-vis private actors following the example of"„collecting societies" in the protection of intellectual property: A model for a net friendly legal instruments

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 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 transsubjective 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 transborder 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. One can even go so far as to assume that networks themselves become quasi-subjects in their own right.

26 In the US eBay offers an electronic mediation procedure via "Square Trade;" http://pages.ebay.com/services/buyandsell/disputeres.html

27 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, 64 Juristenzeitung 961 (2009) with a comment by Karl-Heinz Ladeur; 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 (Yale UP, 2008), 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".

28 Harrison C. White, Identity and Control: How Social Formations Emerge 345 (2nd ed., Princeton UP, 2008).

29 Karl-Heinz Ladeur, *Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken,* 24 Datenschutz und Datensicherheit 12 (2000); for a critique to "economization" of data following the model of intellectual property rights, see Thilo Weichert, *Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung,* 54 Neue Juristische Wochenschrift1463 (2001).

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

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

4.1 From organized criminality toward "criminal networks" – the example of Al Khaida

On February 27th, 2008, the German Federal Constitutional Court[31] pronounced a new fundamental decision on online investigation for the purpose of criminal prevention. It has pronounced a new "computer freedom"[32] 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 *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[33] 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. [34] 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[35] 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 Khaida[36] 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), 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[37] we have networked criminality.

31 Federal Constitutional Court (BVerfG), 61 Neue Juristische Wochenschrift 822 (2008).

32 See the comment by Martin Eifert, *Informationelle Selbstbestimmung im Internet*, 28 Neue Zeitschrift für Verwaltungsrecht 521 (2008).

33 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).

34 BVerfGE 85, 386; see generally A. Michael Froomkin, *Legal Issues in Anonymity and Pseudonymity*, 15 The Information Society 113 (1999).

35 BVerfG, 61 Neue Juristische Wochenschrift 822 (2008).

36 See RAND Document *"Beyond Al-Qeida,"* 2 Vols., 2006.

37 Manuel Castells, The Rise of the Network Society, Vol. 1: Economy, Society and Culture (2nd ed., Willey-Blackwell, 2000).

As in franchising networks[38], 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" that indicate imminent danger. 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.

There is a deep imbalance between the rights of users and third parties – private and public – in the online world: In the offline world the state, in particular, 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 *e. g.* by telephone.[39] If, however, the collection of proofs meets a systematic difficulty linked to the whole technological structure of the online world, this could 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 as defender of individual rights. 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. However, 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.*).[40] 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. This means, that the fragmentation of the "internet fora" which replace traditional conceptions of a publicity that is managed by the classical media risks to sever the public debate as a means of rationalization of politics, reflection of individual motives or reciprocal observation and evaluation of behaviour.

4.2 Criminal procedural investigation

There is a lot of discussion about data-protection by technology – so why not think about a technology that would not protect privacy in a fundamental way but would impose limits on the use of procedural measures ofpublic 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"

38 Gunther Teubner, Networks as Connected Contracts 21, 235 (Hart Publishing, 2011).

39 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).

40 See the overview in Mark A. Graber, Transforming Free Speech: The Ambiguous Legacy of Civil Libertarianism 144 (University of California Press, 1991).

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").[41] 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 under certain conditions to make a link between the online and offline worlds, *i. e.* the real person and its avatar.[42]

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.

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.)

5. Contracts on the use of social media as „networks of contracts"?

5.1 Social media and data protection

The use of "social media" such as *Facebook* has raised several legal questions, of data protection, in particular. This problem will exacerbate in the future because – as has been shown by *Facebook*'s entry on the securities market – the high value of a firm such as *Facebook* is, to a large extent, a valuation of hope. The actual profit drawn from personalised advertising does not yet justify the actual value of the firm.[43] This is why conflicts concerning data protection are gaining more relevance. The firms have to develop more novel forms of advertising, an evolution which, in turn, raises more concerns about the protection of privacy because "social media" promise more fine-tuned addressing of advertising, and this includes more observation of user- habits and interests. Both the data protection officers of the German *Länder* and a recent court judgment from the Berlin District Court (*Landgericht*)[44] have raised concerns about *Facebook*'s practices of both the collection and the use of personal data for advertising purposes. In the context of a constitutional perspective on the conflicts concerning new electronic media in general, the question should be asked as to whether or not new trans-subjective institutional solutions could be formulated in order to attempt to bear in mind the deep transformation that is taking place in the new media. Both the firms themselves and the protagonists of a more rigid conception of data protection tend to focus on the role of the consent of the individual consent (the will of both the users and the providers) or the individual interest (mainly) of the users.

41 BVerfG, 61 Neue Juristische Wochenschrift 822 (2008).

42 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); *id.*, *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 128 at 159 *et seq.* (2004).

43 http://www.forbes.com/sites/petercohan/2012/05/10/can-facebook-tap-11-billion-mobile-ad-market-to-justify-pe-of-206/

44 LG Berlin, judgement of March 6th, 58 Wettbewerb in Recht und Praxis (WRP) 623 (2012); cf. Christian Solmecke/Annika Dam, *Wirksamkeit der Nutzungsbedingungen sozialer Netzwerke*, 15 Multimedia und Recht (MMR) 71 at 732 (2012) (Facebook).

This is all the more problematical as the right to privacy is in itself a right that lacks transparent contours like a classical liberal right,[445] and seems to be dependent on the individual self-interpretation of the users. Recent empirical analyses tend to come to the conclusion that there is a wide range of attitudes towards the protection of private data with regard to the diffusion of news among "friends". At the same time, there have been protests on the part of the users against one-sided changes of privacy rules set up by *Facebook*, for example. The inherent dynamic of transformation of social media leads to a complexity of the rules and patterns of communication[46], and to their re-coding for commercial purposes, which is not easily accessible to individual users. One could think about a more "trans-subjective" approach to privacy in social media that would include a more institutionalised conception.

This could look plausible because the right to privacy as a new right beyond the realm of classical liberties could be attributed to the new "risk based law" – as opposed to the classical right of being protected from "danger" - as is the precautionary principle in environmental law whose individual component is also only mediated. In data protection law, this seems to be similar.[47] This is why there is a need for more trans-subjective institutions that are better adapted to the process, such as distributed interest in the control of the "re-coding" and "re-profiling" of data. This assumption is not equivalent to a fundamental break with classical doctrine, but it should open a perspective on the development of a "conception", which would allow for experimentation with the instruments which the current legal system contains, and would opt for public intervention only in a limited way – because of the uncertainties of the markets.

5.2 The „network contract" as a new paradigm of private law for the „social media"

First of all, it should be recognised that, besides other legal arguments for the liability of social-media providers, primarily the relationship between users and social media is a contractual one. In the American literature, this type of contract is regarded as an "*adhesion contract*".[48]

In legal practice, this means that the contract has the legal value of a more or less one-sided submission to the contract because conditions are normally formulated by only one partner of the contract, *i.e.*, the "provider". The construction of a contractual relationship seems to be adequate because one partner, the provider, offers the possibility of using the communication services, whereas the other, the user, gives his consent to the use of the data that he places on his account for advertising strategies. This mutual consent brings about a relationship of reciprocity: the user can expect the conditions of use not to be changed arbitrarily. The provider lays open the conditions of use and the commercial use of the data for advertising, in particular. An exclusion of any forms of advertising is not a choice which is open to the users.

The specific contractual relationship that is brought about in this constellation is characterised by the fact that a high number of similar "exchange" contracts are concluded at the same time, and that conditions of use are formulated by the provider. However, at the same time, there is a second level of inter-relationships among the users themselves, which is not just a multiplication of a standardised version of a contract, although, in this

45 This is why Helen Nissenbaum's conception of "*Privacy as Contextual Integrity*", 79 Washington Law Review, 119, at 136-8 (2004), does not look promising because contexts are so varied; see, also, the critique by James Grimmelmann, *Saving Facebook* 94 Iowa Law Review, 1137, at 1169 (2009); whereas in the public-private relationship the idea of "relational surveillance" that might have a "chilling effect" on the use of the freedom of association (and freedom of opinion) as Katherine Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance,* 49 Boston College Law Review, 741 (2008), the effect of private collection of data on the rights of users is far from obvious (which does not mean that it is non-existent).

46 Arun Mal & Jenisha Parikh, *Facebook and the Right to Privacy: Walking a Tight Rope*, 4 National University of Juridical Studies Law Review (NUJS LR), 299 at 305 (2011); Helen Anderson, *A Privacy Wake-Up Call for Social Networking Sites?*, 20 Entertainment Law Review, 245 (2009), refers to a practice of users to allow for the use of „their" data by inadvertently neglecting their privacy settings.

47 Cf. Karl-Heinz Ladeur, *Das Recht auf informationelle Selbstbestimmung – eine juristische Fehlkonstruktion?*, 62 Die Öffentliche Verwaltung 45 at 48 (2009).

48 Cf. the seminal article by Friedrich Kessler, Contracts of Adhesion – Some Thoughts About Freedom of Contract, Yale Faculty Scholarship Series Paper 2731, http://digitalcommons.law.yale.edu/fss_papers/2731.

case, the relationships between the participants including the user – user-relationships - form a "triangular" contract. The consent of the user to make use of the data for advertising only makes sense in the event that the other users allow for this use, too. This constellation might allude to the recent construction of "network contracts"[49] – with a principled construction of this new type of contract, although Stefan Grundmann is more prudent in this regard.[50] The sense of such a construction could consist in the consequence that the triangular nature of the contract does not remain at the factual level but can lead to ideas about a specific "hybrid" institutional component. The relationship is a "hybrid" one in as much as it can be located beyond the level of the bilateral exchange contract, but below the level of a "company" (or, even less so, a corporate association). One has to bear in mind that this is not a normal case of a pre-determined setting of "general terms and conditions" that supplement the consent of the partners on the reciprocal rights and obligations, but of a one-sided competency of the provider to define the main duties of the user and to change them whenever he deems it appropriate.[51] The differentiation of the informational scheme of *Facebook*'s sites mirrors, in a way, the "hybrid" character of the "regulatory" structure of the network: *Facebook* has, apart from the site on which the general terms and conditions are laid out,[52] a separate site on "governance",[53] which contains rules of procedure on the change of rules, *etc*. This construction might look promising, although, as a consequence, only those members that click on this site[54] obtain the information on the procedures.[55]

The trans-subjective ("hybrid") component of the contract is to be seen in the fact that the purpose of the contract is not to be formulated clearly in advance. The relationships within the network are prone to continuous change, they evolve upon the basis of communication processes, which, first of all, are freely formulated and are integrated into a vast open network of relationships that allow for a plethora of communicative options. It is only at a secondary step that the provider observes these inter-relationships and tries to design the possibility of "surfing" on this network with the modelling of a commercial type of interest.

Advertising in the "social media" does not follow the traditional patterns of addressing a mass public; instead, it is characterised by the observation and "appropriation" of specific communicative networks that are spontaneously generated by the users. These differentiated networks process personalised information on consumer interests that may be re-coded by advertising firms. This is also the reason why the consent of the users for the re-processing of personalised profiles cannot be determined in detail *ex ante*.

This new constellation might fit into the new framework of "networks of contract" which might help develop new rules for the management of a hybrid "network interest" (G. Teubner) between exchange and collective interests. This "network interest" is emergent and heterarchical; at the end of the day, it can only be adopted for purposes of advertising if this is consented to by the users. The provider cannot just follow his own interest, but also has to support the processing of the networks of communications between the users by shaping an adequate institutional framework.[56] The relevance of the network of the inter-relationships *between* the users and the openness of the experimental development of communicative patterns and, at the same time, the evolving possibilities of personalised advertising could be a sound basis for the re-formulation and concretisation of the pre-conditions of "informed consent" in a dynamic environment.[57]

49 Teubner, *supra* note 40.

50 Stefan Grundmann, *Die Dogmatik der Vertragsnetze*, 207 Archiv für die civilistische Praxis, 718, at 757 (2007).

51 For a critique, see Robert J. Ferenzi, *Friending Privacy: Toward Self-regulation of Second Generation Social Networks*, 20 Fordham Intellectual Property, Media and Entertainment Law Journal 1049, 1056 (2010).

52 www.facebook.com/legal/terms.

53 www.facebook.com/fbsitegovernance.

54 Recently, *Facebook* has announced a change in the "terms of use" on the governance site and opened a voting procedure for the week of 1 June to 8 June 2012; however, only a tiny fraction of the users that remained far below the quota has participated; cf. "Die Mitbestimmung ist rein virtuell", *Frankfurter Allgemeine Zeitung* of 6 June 2012.

55 See Ferenzi, *supra*, note 51, at 308.

56 This complex new network related interests might also give an explanation for the fact that apparently the interests of the individual users concerning their "own" data seem to be limited, as Grimmelmann, *supra* note 45, at 1182, rightly assumes; see, also, *idem*, *Privacy as Product Safety*, 19 Widener Law Journal, 795 at 795-97 (2010).

57 Rebecca MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom 243 (Basic Books, 2012) and passim;

5.3 Proceduralisation of „informed consent"

In order to do justice to the emergent character of the rules[58] and patterns of communication and their re-coding by advertising strategies, one might think about introducing a procedural format that has been used in regulation in conditions of complexity, *i.e.*, the "notice and comment"[59] procedure which the new rules given by the provider should be required to undergo.

This is a new institutional requirement of norm-setting in public procedures. However, it could also be transferred to private processes that have to observe and aggregate the knowledge that is distributed over a high number of users and considers both the normative expectations and the social norms generated over the networks of communication in a process of private norm-making. This procedure seems to be specifically adequate in conditions of a modelling in conditions of complexity. One should think about a transfer of this format at least to contracts on the use of social media. As a procedural element of rule-making, it has not been confined to regulation in domains of public law: in globalised private rule-making[60] , it is quite common to make use of "notice and comment" as a requirement of the adequate balancing of interests.[61] The process of communication within the networks of social media is also a source of new social norms[62] concerning privacy expectations, the limits of intimacy and secrecy, of fashions and habits, *etc.*,[63] which are re-coded by new forms of personalised advertising, and which might become the object of supplementary "web obligations".

The formation of norms through a spontaneous emergence of patterns of communication and their stabilisation through social expectations and norms and their use in advertising strategies all play an important role in social media. This could be regarded as a "network effect" that might be attributed legal value. A legal "network interest" could be formulated in as much as the provider could be come the addressee of a procedural obligation to formulate "net friendly" norms that are open towards the experimentation with new forms and norms of communication and to ascertain a level of reflexivity within the "network of contracts".

Through the architecture of the user formats and the „terms and conditions of use" that are formulated by him, the provider creates the institutional basis whose relevance extends far beyond the narrow limits of an exchange contract. As in the classical media (press, broadcasting, *etc.*) a public interest concerning

the dynamic of the social media is also emphasised by Grimmelmann, *supra* note 45, at 1195; the District Court of Berlin (*Landgericht*) has taken the view that several of the clauses contained in the "Declaration of Rights and Obligation" (German Version) are not in conformity with the German law on the use of clauses on "terms and conditions" in contracts and cannot be regarded as being included in the contract.

58 This transsubjective relevance of rules that are generated in the networks of communication is a focus in Strahilevitz, *supra* note 7, at 925-7 (2005); the networks as such have to be integrated into the legal system not just the protection of individuals in multifaceted "contexts".

59 Cf. Ferenzi, *supra* note 51, at 1100; the specific problems of accessing "terms and conditions" in the internet to regard "click through" bettings or a "browse wrap agreement" as being appropriate as procedure of information and as a consequence a "clicked" consent also being "informed" shall only be mentioned, cf. Ferenzi, *supra* note 51, at 1072-75 & 1078; see, also, *Fteja* v. *Facebook, Inc.*, No 11 Civ. 918 (RJH), 2012 (WL 183896) SDNY, 24 January 2012; for a new informational approach to privacy also Joseph M. Reagle jr., P3P and Privacy on the Web FAQ, http//:www.w3p.org/P3P/P3FAQ.html.

60 Cf. only the contributions in Walter Mattli & Ngaire Woods (eds.), The Politics of Global Regulation (Princeton UP, (2012).

61 The integration of changed "terms and conditions" into a contract via internet communication ("browse wrap agreement") pre-supposes already according to court practice in Canada "reasonable notice" (*Kanitz* v. *Rogers Cable Inc.*, (2002), 58 O.R. (3d) 299 (Ont. Sup. Ct.); this implies an obligation imposed on the user to check from time to time whether changes have been posted, and not an explicit "I agree" communication; the postion of US courts is quite similar: *Register.com, Inc.* v. *Venlo, Inc.* 356 F. 3d. 393; 2004 US App. LEXIS 1074 69; USP. Q.2D (BNA) 1545.

62 Interestingly *Facebook Inc.* itself observes and refers to the emergence of "social norms" in social media according to which the users do no longer value privacy in the traditional sense, as Mark Zuckerberg, *Facebook*'s founder declared, www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

63 This includes the use of biometric data ("autotagging" for "Facial recognition"), a practice that has been criticised by the Irish Data Protection Officer in the "Report of Audit" on *Facebook Ireland Ltd.*, 21 December 2012, in spite of the fact that this issue is not specifically addressed in Irish data-protection law, available at: http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf.

the functioning of societal communication versus the stateis at stake. At the same time, it is increasingly recognised that - as a kind of reverse side of the protection of communication - an institutional self-limitation against a potential self-endangerment of its function appears to be necessary. This seems to be all the more so because it is the user-generated content,[64] and not just the use of pre-determined information, that makes the difference[65]: this situation creates a lock-in effect because the user cannot easily transfer his content to a different network. The specific "web interest" that goes beyond exchange interests demands a type of self-regulation by the provider – this type of self-regulation of a whole *group of firms* can be found in the laws on the protection of minors in public, for example, in Germany. However, there is no reason why regulation of self-regulation should not be extended to single (powerful) firms. In the past, "self-regulation" was primarily regarded as an alternative to public regulation.

In the meantime, however, a kind of "regulatory private law" – to name only consumer protection law[66] – has also emerged, which, in contrast to competition law and its focus an the preservation of markets, aims at a direct steering of behaviour with a view to the creation of more variety of choices beyond the traditional narrow control of contracts. A new private-law based construction of the emerging figure of a "network contract" on the use of "social media" could be a new case for the conception of private regulation if one also takes into consideration the impact of a public interest in new hybrid versions of "private public" communication. [67]

The "notice and comment" procedure could be such an element of regulation in the forms of private law. At the same time, one could go a step further and impose a duty on providers to support the the mediation of interest between the firm and the users. These mediators could help the users to participate in the "notice and comment" procedure in a meaningful way.[68] It has to be borne in mind that the fragmentation of the forms of use, the novelty of the emerging personalised strategies of advertising and the complexities of the "network contracts" including the difficulties in understanding the consequences of the position of individuals in the overlapping networks of inter-relationships are a good reason to think about the protection of a new type of "consumer" *i.e.*, a hybrid type of "netizen", who plays different roles in the dynamic evolving web. A supplementary reason for public intervention could be seen in the fact that, from case to case, the interest of the user might be of only low relevance, and this might block access to courts for factual reasons, whereas the public interest of allowing conflicts about data protection to be brought to court is considerably higher.

5.4 The impact of constitutional law on private „network contracts"

In many European countries, this idea could be linked to the conception of the impact of constitutional liberties on private law, on the one hand,[69] and the procedural dimension of the protection of civil liberties, on the other. This latter dimension has, until now, been considered only for public law, *i.e.*, the German Fed-

64 The protection of user generated content is an element that could also be given more contours if it was more related to the productivity of the networked communication and would not only be regarded as „property" of an individual user: it is content that is generated over the network and should not be easily be attributable by „informed consent" in a formal way to the service provider; see, only, Ferenzi, *supra* note 51, at 1064; see, also Mal & Parikh, *supra* note 46, at 302, who rightly refer to the fact that the fact that more often than not "content" is distributed over various *Facebook* sites.

65 In Germany, the District Court of Berlin (*Landgericht*) in a judgment of 6 March 2012 - judgment No. 16 O 551/10 – published in: 58 Wettbewerb in Recht und Praxis, 613 (2012) has declared the broad reservation of competencies to make use of user generated content in particular has been regarded as being incompatible with data protection law and with the requirement to restrict the breadth of transferred intellectual property rights.

66 Eva Kocher, Funktionen der Rechtsprechung. Konfliktlösung im deutschen und englischen Verbraucherrecht 477 (Mohr, 2007).

67 Zittrain, *supra* note 27, at 213.

68 For the necessity of transparency of terms of use, see the above-mentioned Irish report, *supra* note 63, at 4.

69 The article by Aurelia Colombo-Ciacchi, *The Constitutionalization of European Contract Law: Judicial Convergence and Social Justice*, 2 European Review of Contract Law, 167 (2006), demonstrates upon the basis of research in ten European countries that the "horizontal effect" of civil rights is widely recognised by courts in Europe; see, also, ead., Giovanni Commandé & Gert Brüggemeier (eds), Fundamental Rights and Private Law in the European Union, 2 vols., (Cambridge University Press (2010).

eral Constitutional Court has, on several occasions, derived a protective,[70] and, in particular, a procedural, component even from substantive civil liberties; at the same time, it has emphasised the constitutional relevance of duties to be heard not only in procedures that aim at a restriction to be imposed on a civil liberty, but also in the case of a right to be protected from harm that is expected from industrial installations (nuclear power plants, in particular).[71] Against this background, only a further step would be needed to combine both the doctrine of the expansion of civil liberties to private law and the procedural dimension of civil liberties, and to regard this as a basis for the development of new procedural requirements for the construction of a new network contract on the use and design of "social media". In collective labour law, procedural elements of the protection of privacy have already been developed.[72] Clearly, one has to bear in mind that *Facebook* is not only a network, but that it is also a transnational network which raises the problem of determining the applicable domestic law.[73] This, however, is a complex question that needs differentiation with respect to public and private law, and will not be tackled here. In a context of international or transnational constitutional law, one could at least consider the possibility of constructing a transnational effect of domestic constitutions in the sense that a domestic constitution should not just simply be "applied" to transnational networks, but its trans-border expansion should take into account that other domestic constitutions are also at issue.[74] This could be a case of heterarchical approach to the constitutionalisation of transnational private law that accepts some leeway for the self-regulation of private actors, and fine-tunes constitutional requirements in a co-operative manner that always considers whether constitutional "irritations"[75] imposed on private legal relationships would be acceptable for other countries and their legal system, as well.

5.5 The creation of "information brokers" and cyber courts" as components of a new institutional architecture of internet governance

Finally, one could go one step further and improve the position of the users and the procedure of consenting to the use of their data in advertising by transforming the rights of the users to their data to a quasi- property-like intellectual property,[76] which could lead to more clarity about the object of the "informed consent" (including a right to financial compensation) and could justify the ability to bring claims to court tocollecting societies as is common in intellectual property law. This task could be transferred to the above-mentioned "information brokers", which need not have a monopoly. They could even develop competing strategies and contribute to a pluralistic conception of the reflection of social media. Such a solution would strengthen the position of the users in the process of formulating and transforming the conditions of use in the social media. At the same time, it would contribute to a strategy of establishing transparency in the networks of contracts and their evolution. In addition to the "proceduralisation" of data protection law outlined in this paper, the development of a more network-friendly "alternative dispute resolution"

70 Cf. the overview in Dieter Grimm, *The Protective Function of the State*, in: Georg Nolte (ed), European and US Constitutionalism 137, at 154-155 (Cambridge University Press, 2005); Frank Michelman, *The Protective Function of the State in the United States and Europe*, in: *ibid.*, 156 *et seq*.

71 Reports of the Federal Constitutional Court (BVerfGE vol. 53, 30, 65 – Nuclear Power Plant Mülheim-Kärlich).

72 Cf. for the role of workers representatives in collective labour law Reports of the Federal Labour Court (BAGE) vol. 127, 276.

73 This is due to the fact that the relationship between "*Facebook Ireland*" and the American organisation is contested: The Irish Data Protection Commissioner apparently takes (with good reasons) the view that *Facebook Ireland Ltd.* is the legally autonomous European branch of *Facebook* and is subject to the control by Irish authorities in the EU; German authorities like the Data Commissioner of the state of Hamburg regard the *American Facebook Ltd.* as the relevant legal actor, and as a consequence assume a competency for supervision of German authorities, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Datenschutz. Tätigkeitsbericht 2010/2011, 2012, p.158-160.

74 Cf. Karl-Heinz Ladeur & Lars Viellechner, *Die transnationale Expansion staatlicher Grundrechte*, 46 Archiv des Völkerrechts, 42 (2008).

75 For the use of this conception that attributes also emergent heterarchical proliferating effects to the law as opposed to a hierarchical construction of a superiority of norms and application or of a ranking of norms, see Gunther Teubner, *Legal Irritants. Good Faith in British Law or How Unifying the Law Ends Up in New Differences*, 61 Modern Law Review, 11 (1998).

76 This construction is not equivalent to protection of data as object of „ownership" right away – a construction that is criticised by Grimmelmann, *supra* note 45, at 1192.

mechanism (that has been modelled for the protection of personality rights in the previous section) should be required also in this domain, which would allow for a simplified (electronic) procedure and decision by a private "cyber court", instead of a decision by a state court.[77] The advantage of such a procedure would not only consist in easing access to the protection of rights, but also primarily in the acknowledgement that postmodern society needs a new institutional infrastructure that is focused on the observation and reflection of rapidly changing social norms, instead of stable legal norms.[78]

The re-construction of the contractual constellation of the operations that are processed in the social media was meant to venture an idea on how a network-friendly development of private law and the institutionalisation of a specific legal regime for the "online world" might be conceived. Unfortunately, many protagonists regard Internet anarchy as the only version of freedom of communication and look wryly at any attempt to establish institutions for free communication. The development of the "social media" demonstrates the ambivalence of such an aversion against legal institutionalisation of the Internet communication. The case that has been discussed here shows that this anarchy might also have detrimental effects on the position of the users of the said social media.

6. Outlook

We need "traffic rules" for the internet and the information society, not the protection 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. The recent discussion about the activities of the US National Security Agency (NSA) that have been disclosed by *Edward Snowden* have provoked a lively controversy in Europe. The frame of reference of the criticism is still the interference with the civil rights of the *individual* of the liberal society and not the collective dimension of *risk* in the society of networks: "Everybody is a suspect!" This is obviously not the case. It is quite plausible to regard the internet not just as a new *means* of communication of the individual but to talk about a new "online *world*" that is related to the "offline world" we are familiar with, but creates new patterns, new social rules and,yes , new pathologies. As has been shown we need a new conception for a law of the "online world", which raises eventually, if one may put it this way, also the problem of managing the conflicts between the two "worlds" and their differing regimes of the "rule of law". We might end up in the development of a new type of a "conflict of norms"-approach that coordinates the two rationalities. First of all, it's time to give the law of the online world contours of its own!

77 This is all the more problematic as according to Facebook's "terms and conditions" (16.1) only the courts of Santa Clara County (CA) shall be competent in cases of legal conflicts. It is dubious, whether this is compatible with European E-Commerce and consumer protection law and the European Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (22 Dec. 2000, OJ L 12, 16 Jan. 2001), Article 16 par. 1 (consolidated version: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001R0044:20100514:EN:PDF).

78 For online dispute settlement in conflicts about consumer contracts see generally Calliess & Zumbansen, *supra* note 21, 157.

Para publicar na revista Brasileira de Políticas Públicas, acesse o endereço eletrônico www.rbpp.uniceub.br
Observe as normas de publicação, para facilitar e agilizar o trabalho de edição.