Law and Internet Governance:

Networked Law and Normativities[*]

by

Pierre Trudel[**]

Summary

Law and Internet Governance: Networked Law and Normativities

ABSTRACT:

Introduction

The definition of norms governing the way stakeholders express themselves and interact on the Internet is strongly marked by the changes the network causes in what we view as possible, legitimate and necessary. The Internet affects perceptions and points of view on the foundations of law's power, what is within its scope, and what seems to escape it. Governance of each and every activities taking place in cyberspace mirrors the networked normativities who characterizes the network itself.

Cyberspace brings together many different legal visions and paradigms. There are significant differences between legal systems and cultures with respect to the way rights and freedoms are understood, their scope and how they are ranked in relation to one another.

In order to gain an effective understanding of law in such a space, we need to envision the forms it takes. In cyberspace, law and other normativities are taking the aspect of a network composed of hubs and relays. In-principle normativity is established in the hubs of normativity resulting from technology, state laws and norms generated by supra-state authorities. Between those hubs of normativity, we must acknowledge the role of relays, which take the form of customs, contractual practices, liability rules, self-regulation and other rules of proximity. Law is thus coming to look more and more like a network composed of hubs of normativity relayed through various media and generating a set of networks of rights. This approach gives us a conceptual framework for studying law and other norms participating in the governance of activities taking place in Cyberspace.

1. Converging and diverging conceptions of norms and Law

Laws apply in the communities that have produced and consented to them, and law has no meaning except with regard to communities of reference. Modern law is founded on the paradigm of the territory-based sovereign state governing all forms of behaviour occurring on the land it controls. Such rules of conduct are generally developed through political debates and reflect cultural features and values. In most legal systems, forms of behaviour and the meaning and scope of rules are measured with respect to the cultures and ethical traditions prevailing in the national community.

By contrast, in cyberspace, different systems of values co-exist. That space has the ability to bring into proximity, in a single place, expressions of values that are important to human beings who are extremely distant from one another. Their conceptions of rights and values are different, not so much in terms of how they are worded, but in terms of the meaning given to the rights that are recognized.

By establishing territorial spaces in a place where national boundaries seem derisory, the Internet blurs many markers. Reference communities are coming to be less national communities and increasingly “users”, who are defined more in terms of their interests, language and the tastes and predilections they share. It is therefore not surprising that we have begun searching for a form of normativity able to respond to the concerns of cyberspace communities instead of those of states and national groups.

The real challenge is now related to the understanding of how laws can be applied in an environment (cyberspace) that is also part of a plurality of social and cultural contexts.

2. The compressing of conceptions

With the advent of a space that seems to escape state boundaries and contain none of the familiar signposts on which the principles and practices of law are based. Different conceptions of what law should be are competing. We can talk about the compressing of legal conceptions.

By favouring a redefinition of reference spaces, the Internet sows the seeds of change in parameters defining the legitimacy of law's action. References to location undergo deep alterations when the Internet comes into the picture. Cyberspace changes the importance of state boundaries, lessening their impact on the interactions that it makes possible. It is therefore not surprising to see a loss of relevance, and even legitimacy, of state law when we are seeking ways to regulate behaviour in virtual spaces.[1]

In cyberspace, limits on rights and freedoms cannot be conceived in the same way as within national territories. There is a consensus on the need to seek synergy between the various sources of regulation likely to apply in cyberspace. Such synergy can be achieved by thinking of cyberspace law in a way that recognizes active hubs of normativity interconnected by relays that ensure the effective application of the norms radiating out of the hubs.

3. The organization of normativity in cyberspace

In cyberspace,[2] normativity is increasingly being developed in networks.

A set of systems of norms applies in cyberspace. To begin with, there is state law. Despite a certain romanticism, which has more or less been abandoned today, it is clear that state law does in reality govern many of the interactions that take place in cyberspace. This is compatible with the advent of network law designed to provide frameworks for activities that cannot be entirely governed by national state laws. Technology and the constraints it imposes are also sources of normativity on the Internet.

A) Hubs of normativity

Cyberspace can be pictured as an interconnected set of interacting hubs of normativity. It is composed of spaces in which norms applying to users prevail entirely, or in part. The norms have power either because of their ability to define, even implicitly, the conditions for engaging in the activities concerned or because a state is practically able to exercise authority.

Cyberspace is also made up of relays through which norms and their consequences are clarified and spread. Rules emanating from hubs of normativity are relayed and disseminated in different virtual spaces, and they either complement other rules from other hubs or compete with them.

1) Systems of state law

States continue to govern activities taking place in cyberspace on a national basis, but, given that cyberspace scorns borders, there are practical limits on the application of national laws. At the same time, the limits set by state law apply on the national territory concerned, but can also apply elsewhere if they are not incompatible with the local law.

In cyberspace, spatio-temporal coordinates are often an unsolved problem. Locations and roles are defined and redistributed in accordance with constraints and circumstances that do not conform to a predictable model. These phenomena result from features of electronic environments, such as the immaterial nature of legal situations, evidential difficulties that flow from that immateriality, and the transborder nature of activities, which means that an act that is considered legal in one country can prove illegal elsewhere.

The international nature of many interactions taking place in cyberspace raises problems that neither contracts between parties nor the law of a single state can solve completely. Depending on the jurisdiction in which one is located, different rules can preside over the interpretation of contracts. This is why we are facing the prospect of acceleration of the ongoing movement towards standardization and harmonization of the rules governing international commercial transactions and, more generally, the circulation of information.

2) The law of the Net

In cyberspace, new communities emerge, as do new borders separating not territories, but “domains”, networks, discussion groups, etc. Some theorists advocate for frankly a-state positions. Drawing attention to the difficulty in applying notions set out in national laws, they proclaim that cyberspace, lacking the geographical and physical markers on which regulations in the physical world are based, must be considered as a separate space, governed by its own legal framework.[3] Others refers to how easy it is in a cyberspace environment for stakeholders to evade the application of rules set out in state laws.

Many notions have been suggested as metaphors for the corpus of cyberspace norms that, in many ways, govern wholly or in part the conduct of activities that take place there. Various analogies have shown that cyberspace law can be seen as similar to environmental,[4] maritime, outer space or Antarctica[5] law, or the Lex Mercatoria.[6] This has led to recognition of a so-called Lex electronica.[7]

3) Normativity emanating from technology

The technological architecture is a component of the legal framework of activities taking place in cyberspace. What is meant by technological architecture is the set of technological elements and artifacts, such as materials, software, standards and configurations, which determine access and entitlement to use of cyberspace resources. Objects have a regulating effect that takes various forms. Architectural elements can include software, such as firewalls and proxy servers. Some states use these resources to control the circulation of foreign content on their national Internet networks.

As an environment made possible essentially by technology, the Internet is a space made possible owing to protocols and other functionalities defined in technical standards. Many organizations participate in defining standards making the interconnection characteristic of the Internet possible.[8] Some are state authorities or international organizations of which states are members. Most are private law entities.

Those entities are mainly composed of specialists in the technologies concerned, and to them we owe the standards that ensure the compatibility of many of the computer devices necessary for communication.

Those rules are not necessarily produced by institutions as such: they result from the ongoing and hoped-for behaviour of cyberspace stakeholders. For example, the technological components and products, such as materials, software, standards and configurations, which determine access and entitlement to the use of technological resources and documents, are created in various locations. Rules are generated when experts unite to agree on the specifications for the technological components of electronic environments.

B. Relays of normativity

Proclaiming rights is not everything: the challenge is to ensure they are exercised effectively. This is why it is important to identify the best means for obtaining effective application in an environment like the Internet. The relays are the various means by which Internet stakeholders receive and implement the norms they consider relevant or compulsory.

For example, an access provider must adopt a policy to determine what to do when it is made aware of illegal content. It must relay the definition of what is understood as and held to be illicit in the "domain" or virtual spaces within which it operates.

Relays can be seen as embodiments of the concept of co-regulation. They result from a dialogue process between different hubs of normativity. They must take cognizance of, recognize and transmit applicable laws, and fill in the holes to ensure they are applied concretely and effectively.

1) Liability of stakeholders

One of the major relays between state hubs of normativity and cyberspace stakeholders is liability rules.

For stakeholders, liability is a source of uncertainty. Those taking part in cyberspace activities do so more or less intensively depending on whether or not they are aware that they will be held liable for the information that they disseminate or help to circulate. This shows the importance of mechanisms that distribute responsibilities among cyberspace stakeholders. In this respect, such mechanisms are important relays of state norms applying to a set of activities.

When harm is caused in cyberspace, and the questions of punishment and compensation arise, state norms are often called in as reinforcement.

However, from the point of view of most cyberspace stakeholders, liability looks like a set of risks that must be managed. Individuals and companies must ensure that their practices comply with the requirements of the applicable laws, and take responsibility for doing so. They seek to manage the risk flowing from their activities by taking precautions to guarantee that they restrict their activities solely to roles compatible with the responsibilities they are ready to shoulder.

In order to manage risk appropriately, it is often necessary to anticipate conflicts and identify, in a context-sensitive manner, the relays for the requirements set by the laws and norms that are likely to apply.

This is how the rules of law are experienced by stakeholders. In order to manage the risks associated with possible conflicts, they must clarify their understanding of the forms of normativity. They do so in rules of conduct addressing, for example, the limits that must be respected when messages are sent. They can also adopt rules and precautions regarding incoming messages.

2) Self-regulation and co-regulation

It is primarily to manage risks and delimit their responsibility that stakeholders establish self-regulatory mechanisms.[9] Self-regulation and co-regulation processes are the main relays for the forms of normativity framing activities taking place in cyberspace. Through these processes, rules of law that are considered relevant to a site or environment are updated, adapted and customized. Such processes can be envisaged as continuing cycles in which the needs and requirements emanating from other forms of normativity, including state laws, are taken into account systematically and in an evolving manner.

It is recognized that the rules of the game for many activities taking place on the Internet must be set, at least in part, by the players themselves. There is a strong trend in the development of electronic commerce indicating that the quality of a site's or environment's rules will be a crucial dimension of its establishment and operation, and a significant factor in its success.

Conclusion

Cyberspace is an interconnected whole composed of interacting nodes of normativity. It is made up of spaces in which norms applying to users are enforced wholly or partly on a networked mode. A set of systems of norms are discussed and applied in cyberspace. In addition to government and private regulations, there are processes designed to provide frameworks for activities that cannot be regulated entirely by territory-based law.

Technology and related constraints are also sources of norms in networks.

All of the norms on the Internet can be described according to a network model. Internet activities are thus governed by a networked normativity the effectiveness of which is largely a function of norms producers' ability to create sufficient risk for other stakeholders so as to motivate them to manage the risk. It is as if the network were a vast environment in which stakeholders generate the risks that they perceive, and then in order to manage their own risks, produce obligations that they spread to those with whom they are in virtual contact.

Legal governance on the Internet develops and functions according to a network model. Stakeholders can increase, transfer and limit risks. The effectiveness of regulation is a function of the real ability to increase the risk of those engaging in dangerous activities and to manage the risk of legitimate users.

[*] Talk given at the Université de Montréal in October 2018.

[**] Professor, Centre de recherche en droit public (CRDP), Faculty of Law, Université de Montréal, www.pierretrudel.net email: pierre.trudel@umontreal.ca

[**] Professor, Centre de recherche en droit public (CRDP), Faculty of Law, Université de Montréal, www.pierretrudel.net email: pierre.trudel@umontreal.ca

[1] Dominique Gillerot and Axel Lefebvre, with the collaboration and under the direction of Marc Minon and Yves Poullet, *Internet: la plasticité du droit mise à l'épreuve*, (Brussels: Fondation Roi Baudouin, 1998), p. 18; Yves Poullet and Xavier Thunis, "Droit et informatique: un mariage difficile", in *Computers and Telecommunications: Is There a Lawyer in this Room?,* (Namur: E.Story-Scientia, 1987), p. 9.

[2] Pierre Trudel, "Quel droit et quelle régulation dans le cyberespace?" *Sociologie et sociétés,* Vol. 32, No 2, Autumn 2000, 189-209. < http://www.erudit.org/erudit/socsoc/v32n02/trudel/trudel.pdf >

[3] David G. Post and David R. Johnston, "Law and Borders: The Rise of Law in Cyberspace", (1996) 48 *Stanford L. Rev*., 1367, p. 1378.

[4] Richard S. Zembek, "Note, Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace", (1996) 6 *Albany L.J. Sci & Tech*. 339, 368.

[5] Matthew R. Burnstein, "Note, Conflicts on the Net: Choice of Law in Transnational Cyberspace", 29 *Vand. J. Trans L.* 75, p. 110.

[6] Trotter Hardy, "The Proper Legal Regime for 'Cyberspace'", (1994) 55 *University of Pittsburg Law Review*, 993 p. 1019.

[7] Pierre Trudel, "La lex electronica," in Charles-Albert Morand, ed. *Le droit saisi par la mondialisation*, (Brussels: Bruylant, Éditions de l'Université de Bruxelles, Helbing & Lichenhahn, 2001), pp.221-260.

[8] Marcus Maher, "An Analysis of Internet Standardization", (1998) 3 *Va. J.L.&Tech*, <http:vjolt.student.virginia.edu>.

[9] For an example of risk management and self-regulation methodology, see: Christophe Roquilly and Jean-Paul Cailloux, *Assurer la sécurité juridique des sites web, audit, méthodologie e-business*, (Paris: Lamy-Les Échos, "Agir en connaissance de cause" collection, 2001).