OBSERVARE
Universidade Autónoma de Lisboa

ISSN: 1647-7251
Vol. 6, n.º 1 (May-October 2015), pp. 86-99

JANUS.NET
e-journal of International Relations

CYBERSPACE REGULATION: CESURISTS AND TRADITIONALISTS

Lino Santos
lino.santos@cncs.gov.pt
Holder of a Master Degree in Law and Security from the Faculty of Law of Universidade Nova de Lisboa. Holder of a Bachelor Degree in Systems and Computer Engineering from the University of Minho. Operations Coordinator at the National Cybersecurity Center (CNCS, Portugal)
.

Abstract

In the amazing *Code and Other Laws of Cyberspace*, Professor L. Lessig writes "that something fundamental has changed" with cyberspace with regard to the state's ability to enforce the law.

On the one hand, the structure and characteristics of cyberspace pose some difficulties related to jurisdiction and the choice of applicable law. On the other, it raises questions about the very concept of sovereignty as we know it.

This paper examines the arguments of those who advocate a regulation of cyberspace on the edges of state sovereignty or within a new concept of sovereignty and capacity to enforce the law, and the arguments of those who reject this exceptional treatment of cyberspace.

.

Keywords:

Cyberspace; Regulation; Self-regulation; Sovereignty; Utopia

How to cite this article

Santos, Lino (2015). "Cyberspace regulation: cesurist and traditionalists". *JANUS.NET e-journal of International Relations*, Vol. 6, N.º 1, May-October 2015. Consulted [online] on date of last visit, observare.ual.pt/janus.net/en_vol6_n1_art6

Article received on March, 31 2015 and accepted for publication on April, 30 2015

CYBERSPACE REGULATION: CESURISTS AND TRADITIONALISTS

Lino Santos

Introduction

There is no doubt that cyberspace has brought about profound changes in the way citizens, organizations and states relate to each other.

The capillarity of Internet, along with its large geographical coverage in terms of access and the advent of the personal computer, gave rise to the globalisation of information and knowledge, creating new spaces for interactivity, sharing and storage of market products, among which we highlight the leisure and culture immersive virtual environments (virtual worlds), the product of information technology-mediated social interactions (social networks), or the place where information is stored and processed (cloud). This diversity of spaces representing the wealth of cyberspace applications is the basis of its success and of the rapid growth of its use.

This group of spaces is based on the global communications system – the Internet - to which information systems and personal electronic devices connect to perform their function. If not originally created for military purposes but certainly developed to be used with that objective, the Internet penetrated the academic network in the late 1980s and quickly took over as a means of mass communication in the mid-1990s. In its military origin, the main concern in the Internet's design was resilience to partial failures[1], resulting in a fully distributed physical architecture and management without any connection with the administrative map of nations.

Soon cyberspace was perceived as a space of freedom, a kind of new global Far West where no state could enforce the law and maintain order. In this context, two opposing academic trends emerged.

The first suggests the failure of the legal system to deal with cyberspace and advocates the creation of new forms of regulation adapted to its specificities.

The second supports a treatment of nonexceptionality regarding cyberspace and argues that the challenges in its regulation are no different from those posed by other areas where there are cross-border transactions.

[1] One of the requirements asked to the creators of the Internet, then called ARPANET, was to ensure tolerance to communication failure between military operational bases in a scenario of partial destruction of their infrastructure. Consisting of a "*web*" of connections among the various "nodes", information within this network should always reach its destination as long as there was a path available to do so, thereby reducing the criticality of each individual "node" for the global context of communications.

This article intends to present and discuss these two currents in the light of developments since their initial formulation, and ascertain whether there is a trend or primacy in the use of cyberspace regulatory mechanisms.

Characteristics of cyberspace

Some characteristics of cyberspace architecture pose serious challenges to the governance of this new medium, as well as to the regulation of the various activities conducted within in. To begin with, cyberspace dramatically increases the speed and amount of communications, while reducing or eliminating the gap between institutions, between individuals or between nations.

Emails or SMS are sent and received almost instantly, photographs, videos and opinion articles are shared and disseminated globally in near real time, buying a book over the Internet is now as easy and convenient as to do it in a bookstore. In this context, cyberspace and the conversion from analog to digital brutally increased the frequency and the speed of some existing unlawful behaviour. Examples include copyright infringement, which has always existed but that digital technologies have facilitated and carried to the extreme.

On the other hand, cyberspace is non-territorial. Unlike natural areas (air, sea, land, and space) where states, within their capabilities, exercise sovereignty and enforce the law within a relatively well defined physical territory, in cyberspace that exercise raises demarcation problems.

In the same vein, B. Posen refers to it as another global common, comparing it to the sea, air and outer space (Posen, 2014: 64). Therefore, classical concepts such as "jurisdiction" or "property" - to give just a few examples - become fuzzy when applied to cyberspace. The provision of online services will hardly ever comply with the legal framework of all the states where they are available[2], creating difficulties in their exercise of sovereignty, starting with the very choice of which applicable law to apply - the law where the service is provided, or the law where the effects are produced?

Finally, this virtual space ensures some degree of anonymity to those using it, which again raises difficulties regarding the allocation of acts performed or the identity of the authors. A Portuguese cybernaut or located in Portuguese territory may use a blog service in the US to slander another Portuguese citizen. This same Internet user can play an online game allowed in the country where the server is located but which is banned in Portugal. He may also remotely practice a profession regulated in Portugal, but which is not regulated in the country where the service is provided.

Cyberspace has also brought about a set of new legal protection objects, expanded the protection scope of some existing ones, and facilitated the emergence of new illegal types. Figures such as digital identity, multiple identities, avatar, virtual money, or Internet domain, and professions such as systems administrator, programmer or blogger, still do not have rules that grant them rights and responsibilities.

[2] J. P. Trachtman states that the big novelty of cyberspace is that “it will lead to more situations in which the effects will be felt in multiple territories at once” (1998: 569).

Similarly, traditional concepts such as privacy had their legal protection range extended to include, for example, the right to be forgotten[3], and actions

classified as unlawful in the context of juvenile pornography have started to include ownership of this sort of material in digital format or merely viewing it. [4] One must also refer the need, perceived early, for the legal protection of actual computer systems that constitute cyberspace to be treated separately in cybercrime law.

These and other challenges were evaluated at the turn of the century by various scholars from the field of law. Discussion then allowed identifying two diverging trends with regard to the regulation of cyberspace.

The first trend believes that some of the distinctive characteristics of cyberspace are sufficient to justify the impossibility of using existing legal instruments and jurisdiction, advocating a new paradigm of cyberspace regulation. Johnson and Post, among others, share this view, defending cyberspace regulation for Internet users through self-regulation (1996, 2002). In turn, Lessig advocates regulation through "code" and cyberspace architecture (1999; in this as in all cases that follow, the translation is mine).

On the other side there are those who argue that the challenges posed by cyberspace to the law are not very different from those placed by other technological developments, and that the transactions carried out within cyberspace are no different from other transnational transactions conducted by other means. The main supporters of this view are Goldsmith (1998) and Trachtman (1998), who reject the exceptionality of cyberspace and defend an evolution within the framework of international law and through strengthening supranational regulatory instruments.

The academic debate around the topic has led JP Goldsmith to dub "regulation sceptics" those who, like Johnson and D. D. Post, emphasize the extraordinary nature of cyberspace and ask for a new regulatory model (1998, pp. 1199). In turn, Post calls “unexceptionalists” (2002: 1365) those who advocate that the problems posed by cyberspace to the state's ability to exercise and enforce the law are not that different or new. Without wishing to sound unkind to the authors, henceforth I shall refer to the former as “cesurists” and the latter as “traditionalists”.

Taking advantage of the distance in time of this discussion, this paper will begin by addressing the arguments advanced by "cesurists" and "traditionalists", and then will analyse the two dominant solutions for a better regulation of cyberspace: self-regulation and the additional supranational approach.

[3] Article 17 of the European Commission’s proposal for the regulation of Personal Data Protection states that “the data subject has the right to obtain from the controller the erasure of personal data concerning him”. See *Proposal for a European Parliament and Council Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general regulation on data protection)*, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf, accessed in September 2014.

[4] See point f) of Article 20 of *Convenção para a Protecção das Crianças contra Exploração Sexual (Convention for the Protection of Children against Sexual Exploitation)*, Resolution of Assembleia da República (Portuguese Parliament) no. 75/2012, of 28 May, stating that “[...] consciously accessing child pornography through the use of communication and information technologies constitutes a crime”.

Cesurism vs. Traditionalism

The term "cesurism" - coined by Herminio Martins (Garcia, 2006) is used here as a reference to a line of reasoning that tends to deal with phenomena as being specific and unprecedented, somehow renouncing time and history. This is precisely the thinking of those who, like Johnson and Post, focus their attention on the novelty cyberspace represents to justify the failure of the current regulation model based on the law and the break with the past.

The argument of the "cesurists" focuses on the non-territoriality of cyberspace and, more specifically, on the fact that clear boundaries are a necessary attribute for effective law enforcement. The relationship between space and law, Johnson argues, has multiple dimensions. On the one hand, it is the law that allows a state to exercise sovereignty and control over its territory - a well delimited space recognized by all - as well citizens to defend themselves from state action. In other words, the border concept works as the limit within which the state enforces its law, as well as the limit outside which citizens are safe from state action[5]. On the other hand, the legal significance of the effects of an action - or absence of it - is the same within the same judicial area and, most likely, different between different legal areas.[6] Conversely, the legitimacy of the law comes from a state's citizens direct or indirect participation in drafting the law, this legitimacy being lost when applied otherwise. Finally, the preventive effectiveness of the law results from prior knowledge of the law applicable to the area where we practice relevant acts, or the law where such acts occur (Johnson & Post, 1996).

Given this relationship between area and law, the "cesurists" argue that the geographical location within known physical limits – borders - is essential to determine the set of rights and responsibilities of legal entities, concluding that cyberspace "radically undermines the relationship between legally significant phenomena and physical location" (Johnson & Post 1996: 1370).

Under this assumption, "cesurists" question the competence of any state to enforce law and justice for acts committed in cyberspace and have reservations about the choice of applicable law. Johnson and Post envision cyberspace as a *single medium*[7], as a new action plan or parallel dimension whose border with our physical world is "made of screens and passwords" (1996, 1367) where, once inside, there are no other barriers. Once inside this cyberspace, communicating with the next door neighbour or someone in the antipodes is exactly the same – actually, there is no concept of antipode within

[5] It is through law that a rule of law state governs the freedoms and responsibilities of its citizens and institutions. The effective enforcement of this regulation is an act of sovereignty.

[6] Once again the call for the principles of a rule of law state, where the law must be equal for all. Obviously this equality applies to all legal objects of that state, since the law can be different between states.

[7] M. Libiki suggests that cyberspace is not a single medium but rather a "multiplicity of media – at least yours, theirs and of the others" (2012: 326). Also L. Strate, in his brilliant article on cyberspace concepts, proposes the existence of a multitude of cyberspaces centred on the experience of each individual (1999). It should also be noted that in the ideological framework of a single cyberspace, the concept of "national cyberspace" commonly used in the various national cybersecurity strategies would not make sense. See *The National Strategy to Secure Cyberspace* (2003), available at https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, accessed in September 2014; *or Italy's National Strategic Framework for Cyberspace Security* (2014), available at http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf, accessed in September 2014.

cyberspace - and the legal framework governing such communication either does not exist or is difficult to identify .

The case which opposed the International League against Racism and anti-Semitism to the US giant Yahoo illustrates these difficulties. In 2000, French citizen Marc Knobel, an activist in the fight against neo-Nazism, found that Yahoo's auction portal was selling neo-Nazi material. Through the aforementioned NGO, Knobel took Yahoo – a company based in California - to court for violation of the French law banning Nazi goods trafficking. The first reaction of one of the co-founders of Yahoo, Jerry Yang, was to consider that the French court intended to impose a judgment in an area over which it had no control. Regardless of this opinion, the trial continued, with the defence focusing its arguments on the technical impossibility of distinguishing what was presented to Yahoo French customers from what was presented to the other ones. For its part, the prosecution defended the sovereignty of the French state to defend itself from the sale of illegal Nazi goods from the United States and to question the reason for the existence of an exceptional regime for Yahoo and cyberspace. The court ruled that Yahoo violated French law and ordered the company to take all necessary measures to dissuade and render impossible French citizens' access to such contents. Yahoo's claim about the technical impossibility of fulfilling the court order, based on the idiosyncrasies of the Internet architecture, was surpassed after several Internet gurus, including Vint Cerf, advanced technical solutions that enabled Yahoo to comply with the court order (Goldsmith & Wu, 2006: 1-10).

In line with Johnson's and Post's argument regarding the uniqueness of cyberspace, authority can only be exercised within a territory. These authors questioned the legitimacy of a nation to regulate activities carried out in another country. They also argue that international disputes over choice of a legal framework can be solved by choosing the framework of the location where the unlawful acts are committed. These assumptions guarantee uniformity, predictability and certainty in the application of laws, which are values of rule of law. However, the above case suggests otherwise and supports the views of the "traditionalists".

As opposed to "cesurists", "traditionalists", whose motto could be "nothing new under the sun"[8], advocate that cyberspace is not an exception. For the "traditionalists",

> *"transactions in cyberspace are no different from cross-border transactions occurring in the real space. [...] Both involve people in real space in one territorial jurisdiction transacting with people in real space in another territorial jurisdiction"* (Goldsmith 1998: 1250).

For J. P. Trachtman, cyberspace is the medium. Conduct still occurs inside a territory, its authors still reside in a territory, and, most importantly, effects, although more dispersed than in the past, also continue to be produced in a territory (1998: 568)[9]. As

[8] Ecclesiastes 1:9 "That which has been, is that which is to be, and that which has been done, is that which will be done, and there is no new thing under the sun".

[9] Trachtman rejects the "cesurist" view about the states' reduced sovereignty as a result of cyberspace: "It is not the state that has died, but the long-moribund theory of absolute territorial sovereignty." (1998: 562)

a result, the existing set of principles and traditional legal instruments are able to solve the problems of choice of law and jurisdiction.

The idea that cyberspace brings nothing new is supported by Goldsmith using the analogy with other communication and transnational transactions contexts. The author accepts that the world is changing and that cyberspace is an expression of this change, but notes that international law has evolved to meet these changes, namely "it is commonly accepted that [in the absence of consensual international solutions] a nation regulates the local effects of extraterritorial conduct" (Goldsmith 1998: 1212) and gives industrial property as an example.

By way of conclusion, the other key idea of the "cesurists" is that the legal difficulties mentioned above, combined with the technical difficulties posed by the characteristics of cyberspace, render it impossible for states to regulate it. For Johnson and Post, cyberspace ''creates a totally new phenomenon that needs to be subject to clear legal rules, but it cannot be regulated satisfactorily by any sovereignty based on the concept of territory'' (1996: 1375). The states' technical and legal inability to exercise their sovereignty over cyberspace will, initially, lead to the emergence of self-regulating mechanisms (1996: 1387).

Traditionalists", in turn, argue that the technology exists and that, as demonstrated in the case involving Yahoo, but also in many cases involving content filtering done for various reasons, states can exercise their sovereignty and protect citizens from offensive content or illegal activities (Goldsmith & Wu, 2006: viii). The information involved in a transaction "appears in a territory, not by magic, but due to hardware and software action located within that territory" (Goldsmith 1998: 1216), so acting on that hardware and software makes it possible to perform the regulatory function.

Self-regulation of Cyberspace

This duality of views over a new issue that has not yet been understood in its fullness is recurrent. Throughout history, the emergence of new technologies has led to stances in support of their uniqueness and future role in breaking with the past and creating a better world - instruments of universal peace - as well as to more conservative views that immediately identify affinities with other past episodes. Armand Mattelart (2000), in his *History of Planetary Utopia*, lists a series of historical examples where the emergence of a new technology has led to the emergence of a liberating hope: the printing press, the telegraph, the railways, or television.

As already mentioned, "cesurists" are convinced that cyberspace is one of those liberating technologies. A technology that is sufficiently different from the real world to prevent regulation of human behaviour in that space from being done through existing mechanisms[10]. Lessig argues that "something fundamental has changed" (1999: 126) to support his thesis that in cyberspace "code is law", while Johnson and Post argue that cyberspace belongs to Internet users and therefore "those who have defined and use online systems have interest in preventing the security of their electronic territory and in preventing crime" (1996: 1383), setting the mood for self-regulation of cyberspace.

[10] Lessig argues that the regulation of human behaviour is achieved through the convergence of four forces – four regulators: the law, the market, social norms and, with regard to cyberspace, architecture (1999).

The idea that cyberspace dilutes the concept of state sovereignty, and also that problems in cyberspace should be left to Internet users, fits perfectly the "Internet-centrism" profile as conceived by E. Morozov (2012). The belief in the liberating effect of the Internet, mainly in the idea that it all comes down to, and that everything can be explained or done via the Internet, enables understanding why Johnson and his supporters defend different rules for cyberspace[11].

The theses of the "cesurists" are clearly part of an Internet euphoria context and did not predict the societal changes triggered by the social networks over the past decade or the concentration of power in the mega corporations in the sector. They fall within the spirit and ideology of the Internet in its beginning and its users' wish to keep it free from regulation and intervention by states or to keep alive the idea that cyberspace "can hold its promise of profound liberating leverage " (Post, 2000: 1439). This wish has been expressed by groups like the Electronic Frontier Foundation, and in manifestos like John Barlow's (1996) *A Declaration of the Independence of Cyberspace*.

In this spirit, Johnson and Post point out some practical examples of self-regulation. The authors suggest that the DNS system – a global system for allocating and managing Internet naming, coordinated by a non-profit international organization called ICANN[12], was being redesigned in a process of self-regulation to accommodate a set of safeguards demanded by the "industrial property" (1996: 1388). Nearly twenty years later, we can evaluate how this process took place. Although DNS management remains in the hands of Internet users, almost all European countries have liberalized Internet domain registration rules, putting more pressure on the management of industrial property rights and creating phenomena such as financial cybersquatting - financial speculation with the most desirable Internet names. There is actually a self-regulation system in this area, according to a model of international best practice. However, this self-regulation proves to be insufficient and resorting to industrial property law to resolve conflicts is recurrent. However, it should be noted that, as suggested by Johnson, some countries created specialized arbitration courts[13] with the needed know-how to address cyber particularities (1996: 1387). With regard to the growing number of unsolicited email messages, commonly known as spam, Post gives another example of self-regulation as a way of resolving concrete cyberspace issues. Post presents us one of several initiatives to create a reputed centralized database for email addresses or email servers (Realtime Blackhole List), remotely powered by volunteers whom he calls activists (2000: 1440) as a good example of self-regulation or of how the network will operate in the future. This group of volunteers establishes, together, a set of rules which all participants in cyberspace adhere to. It is indeed a beautiful ideal, but which history has not confirmed. Firstly, not one but several similar initiatives have emerged, creating a problem of choice for email services administrators. Then, the volunteer system has become a constraint in terms of the

[11] "Internet-centrists like to answer every question about democratic change by first reframing it in terms of the Internet rather than the context in which change is to occur" (Morozov, 2012: xvi). One of Morozov's favourite targets is North American writer Clay Shirky, (2009), who he describes as cyber utopian.

[12] *Internet Corporation for Assigned Names and Numbers*. See https://www.icann.org, accessed in September 2014.

[13] In Portugal's case, the rules for the registration of Internet names includes the possibility of appealing to a specialized arbitration court See .PT Domain Registration Rules, Chapter VI, available at http://www.dns.pt/en/domains-2/domain-rules/chapter-vi/, accessed in March 2015.

quality of service, for which reason it led to the commodification of some of these services - the current model[14]. Furthermore, other forms of solving the spam problem have arisen. The market saw the opportunity and cloud giants like AO, Microsoft and Google created the Sender Policy Framework, Sender ID, or the DKIM - to name only the most well-known – so the "collective consensus "advocated by Post (2000: 1456) does not exist, to date. In short, as far as the treatment of spam is concerned, we can say that we suffer from "too much" self-regulation.

In another perspective of the meaning of self-regulation, Lessig's thesis about the code's role in cyberspace regulation is ambivalent. On the one hand, it supports the idea that the production of the standards governing cyberspace lies in its architects and programmers rather than the state. In this scenario, the regulatory power is both in the hands of the telecommunications industry and those of the media and Internet applications industries, which through their products govern and shape behaviours in cyberspace. By keeping untouched the principles of net neutrality and the non-duty to watch over the contents transmitted through or stored in their infrastructure, digital media giants have been introducing in their applications reporting mechanisms for the removal of offensive content or reputation mechanisms for risk assessment in commercial transactions between strangers. On the other hand, creating norms also lies in the hands of ordinary people, who can create a new application and thus produce standards. In both cases this form of producing standards may conflict with other regulatory authorities. Good examples of this self-regulation include: Skype, a global system for voice communications created by two Nordic young people outside the regulatory framework for telecommunications and which violates criminal law provisions in various jurisdictions, such as the telephone interception regime; or the Pretty Good Privacy, an encryption platform developed by Phil Zimmermann, who infringed, among others, the US law on the export of encryption algorithms. On the other hand, Lessing's thesis defines code as the means to comply with the law in a more effective way:

> *"code displaces law by codifying the rules, making them more efficient than they were just as rules"* (Lessig, 1999: 206).

In other words, the state can take advantage of code to exercise its sovereignty. Just as companies have codified their business processes, reducing arbitrariness and employee error, states are beginning to codify some of their functions - particularly those where interaction with citizens is required - with efficiency gains. The current model of tax collection in Portugal is an example of this, where codifying traders' behaviour to issue invoices and codifying taxpayers' behaviour for completing their tax returns constitutes the very law, with the term "statement" starting not to make sense. In the opposite direction of self-regulation, cyberspace architecture also created a set of opportunities for the control and surveillance of society. Authoritarian states were the first to realize this possibility[15], but quickly passive surveillance, indiscriminate

[14] The business model of many of these RLBs involves charging a fee for removing entries from the list.

[15] Perhaps the most obvious example of this control is the *Great Firewall of China*, which is a technological infrastructure allegedly able of monitoring and selectively blocking communications and content within Chinese cyberspace and between the latter and the rest of the world, a kind of virtual censorship "blue pencil" operating in real time.

collection of metadata and the concept of big data in supporting the functions of sovereignty attracted supporters all over the world. States have realized that for better control of cyberspace - theirs and of others, as MC Libiki (2012) put it - the major Internet industry companies can play a key role, whether in the architecture of information flows' topology or in the design of the service's specific functions. To give just one example, the physical location of the Google global search engine is geopolitically relevant. This strategic interest thickens up when we talk about information storage. For example, in the dispute between Google and the government of the PRC in 2010, the latter saw the former as a component of American power (Klimburg 2011: 52).

Disaggregated sovereignty

Aware of the limits of the cyberspace self-regulation process, several authors suggest that traditional regulatory mechanisms should be complemented by a supranational approach to more complex problems. In a more traditionalist perspective – the one that does not advocate an exceptional regime for cyberspace – sharing power with other institutions to better meet the various challenges of global governance, not just those posed by cyberspace, is commonly accepted. The best known examples of this network governance are the various institutions of the United Nations, such as the World Health Organization or the World Trade Organization.

These response structures to contemporary problems of transnational governance have been theorized, among others, by WH Reinicke, who named them "global public policy networks" (1999) or by A.M. Slaughter, who called them "disaggregated sovereignty" (2009). The objectives of these networks fall within the concept of soft-power and determine the transposition of the concept of sovereignty centred on the administration of the territory into a combination of powers established in the states and supranational decentralized mechanisms for coordination among them. These mechanisms are based on structures that bring together the stakeholders – from the government, the economy and also from the civil society - to take advantage of the benefits of networks in knowledge management, to share information and ideas and to coordinate policies among themselves without the negotiated formal nature of a treaty (Mueller, 2010: 40). These forms of government coincide with the concept of multi-stakeholder approach advocated, for example, in the Internet Governance Forum, or in the various working groups of the European Union.

Supporters of this approach do not see it as a loss of state sovereignty, but as inevitable for solving global problems. As Slaughter states,

> *"however paradoxical it sounds, the measure of a state's capacity to act as an independent unit within the international system – the condition and objective of sovereignty – depends on the breadth and depth of its links to other states"* (2009: 268).

Cyberspace's regulatory problems are no exception to this rule. As stated by JS Nye Jr. (2010: 3),

> *"cyberspace will not replace geographical space and will not abolish state sovereignty, but the diffusion of power in cyberspace will coexist and greatly complicate what it means to exercise power along each of these dimensions".*

In this regard, various authors advocate a global solution to a global problem. HH Perritt Jr. suggests that

> *"taking into account the potential of [cyberspace] requires an evolution of international public and private institutions so that the rules for responsibility assignment can be enforced effectively, even in relation to conduct that cannot be located territorially in a particular state"* (1996: 113).

Trachtman also insists that "it is worth devising a stronger institutional solution" (1998: 569) for the regulation of cyberspace.

One area where this disaggregated sovereignty has been producing effects is in fight against cybercrime. The need for a transnational approach to the challenges posed by crime in computer networks was perceived very early. In 1990 the United Nations General Assembly adopted its first resolution on the need to develop international cooperation forms and instruments for combating cybercrime[16].

Again within the United Nations, the 11th Congress on Prevention and Criminal Justice held in 2005 produced a declaration expressing the need for legislative harmonization in the fight against cybercrime[17].

This objective was attained in 2004 at the meeting of the G8 Ministers of Interior held in Washington, which produced an action plan to combat high-tech crime, encouraging all countries to adopt the Convention on Cybercrime of the Council of Europe, 2001[18].

This Convention is often referred to as the first international working document resulting from deep reflection on the subject (Verdelho et al., 2003). One of its main objectives is to harmonize the various national laws concerning crimes committed

[16] Resolution A/RES/45/121, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, available at http://www.un.org/documents/ga/res/45/a45r121.htm, accessed in May 2014. This resolution resulted in a guide on the prevention and control of computer-related crimes. See *United Nations Manual on the Prevention of Computer-related Crime*, available at http://www.uncjin.org/Documents/irpc4344.pdf, accessed in May 2014. In 2000, the same Congress adopted a new resolution on fighting the criminal use of information technologies, reinforcing the need for member states to ensure that legal systems did not create free zones for the exercise of this type of criminal activity and calling for increased transnational criminal and legal cooperation. See Resolution A/RES/55/63, *Combating the criminal misuse of information technologies*, available at http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf, accessed in May 2014.

[17] See *Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice*, "Bangkok Declaration", available at http://www.unodc.org/p df/crime/congress11/BangkokDeclaration.pdf, accessed in May 2009.

[18] Full text available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, accessed in May 2009. For a summary on the origin and objectives of the Convention on Cybercrime, see http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm, accessed in May 2014.

against computer networks or content crimes in computer networks. In addition to the criminal law, the Convention also aimed at a more effective transnational cooperation, contributing to that effect with a set of criminal procedural law institutes and the creation of instruments for transnational judicial cooperation.

Also in the context of the United Nations, some unsuccessful attempts were made to conclude an agreement to limit the use of cyber weapons by a state. Due to distrust in the efficacy of such an agreement, in particular regarding the possibility of checking it, or simply because there is no strategic advantage for the US, this country has consistently rejected this agreement (Clark & Knake, 2010: 219-225).

In the same direction and in response to the growing centrality of cyberspace in terrorist activities, either as an instrument or as a potential target, the European Union is about to adopt measures to better control and monitor jihadist activities on the Internet. Among these, the creation of a special unit within Europol stands out, with a view to monitoring the Internet and strengthening public-private cooperation with social media major giants such as Facebook or Twitter, to ensure the effectiveness of such monitoring[19].

Another example of disaggregated sovereignty for better regulation of cyberspace will arise with the new EU directive on network and information security which, predictably, will also be approved in 2015. The draft directive[20] includes the creation of *fora* to share information and best practices, to combine efforts in response to cyber security incidents and strengthen the relationship between national cybersecurity authorities, in a multi-stakeholder approach.

Conclusions

Repeatedly, the emergence of a new technology has originated stances in support of its exceptionality and break with the past. As suggested by Trachtman,

> *"perhaps because the technology is so exhilarating, there is a tendency to claim that the changes we do observe in sovereignty, the state, jurisdiction, and law all are caused by cyberspace"* (1998: 561).

The same had happened with the advent of the telephone, the telegraph and radio.

Much of the difficulties in regulation and law enforcement in cyberspace are due to profound changes in society - catalysed by that very same cyberspace - such as the deepening of globalization and the consequent increase in cross-border transactions or the speed of technological development. On the other hand, cyberspace has distinct and ambivalent features that pose great challenges to states in terms of its regulation,

[19] See *EU proposes terror unit to tackle online jihadism*, Financial Times, 11 March 2015, available at http://www.ft.com/intl/cms/s/0/4d93b7f0-c804-11e4-9226-00144feab7de.html, accessed in March 2015.

[20] See *COM(2013) 48 final, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:PT:PDF, accessed in September 2014.

but also opportunities for greater surveillance of society. Therefore, we are not faced with an exceptional problem, but rather with a libertarian, economic and political opportunity for the various stakeholders involved.

After almost twenty years after the work of Johnson and Post, *Law and borders: the rise of law in cyberspace*, the path set for its regulation is not absolutely clear. Depending on the interests of each state (economic or security) we have situations where greater self-regulation (economic interest) prevails and others where there is growing surveillance and control of society (security interest), resulting in the fragmentation cyberspace into cyberspaces.

We can also say that under these two trends, cyber-utopianism is exactly that: utopia.

> *"It's too easy to argue that the regulation of cyberspace belongs to the cyberspace society."* (Trachtman 1998: 568)

The two approaches examined here - self-regulation and disaggregated sovereignty - coexist and most likely will continue to coexist. As stated in the chapter on guiding principles of the 2011 Dutch Cybersecurity Strategy: "Self-regulation if possible, legislation and regulation if necessary”[21].

Finally, and considering the difficulties discussed here for a state to carry out, *per se*, this regulation, we observe the emergence of transnational governance networks and the strengthening of their role on the political agenda. The concept of absolute sovereignty centred on the administration of the territory is becoming diluted and global issues are addressed in these transnational structures. A global approach to global problems is required.

References

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Disponível em https://projects.eff.org/~barlow/Declaration-Final.html, consultado em Setembro de 2014.

Clark, R. A. & Knake R. K. (2010). *Cyberwar – The next threat to national security and what to do about it.* New York: HarperCollins

Garcia, J. L. (2006). Introdução: Razão, tempo e tecnologia em Hermínio Martins. In M. V. Cabral, J. L. Garcia, & H. M. Jerónimo (Eds.), *Razão, tempo e tecnologia: estudos em homenagem a Hermínio Martins* (pp. 13– 47). Lisboa: Imprensa de Ciências Sociais.

Goldsmith, J. L. (1998). Against cyberanarchy. *The University of Chicago Law Review*, 65(4), 1199–1250.

Goldsmith, J. L. & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. New York: Oxford University Press.

[21] See *The National Cyber Security Strategy (NCSS)*, available at https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011, accessed in September 2014.

Johnson, D. R. & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48, 1367–1402.

Klimburg, A. (2011). Mobilising cyber power. *Survival*, 53(1), 41–60.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic books.

Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *I/S: A Journal of Law and Policy for the Information Society*, 8, 321–336.

Mattelart, A. (2000). *História da Utopia Planetária*. Bizâncio.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York: PublicAffairs.

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. Mit Press.

Nye Jr, J. S. (2010). *Cyber power*. Technical report, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Perritt Jr, H. H. (1996). Jurisdiction in cyberspace. *Villanova Law Review*, 41(1), 1–128.

Posen, B. R. (2014), *Restraint: A New Foundation for US Grand Strategy*. London: Cornell University Press.

Post, D. G. (2000). What Larry doesn’t get: Code, law, and liberty in cy- berspace. *Stanford Law Review*, 52, 1439–1459.

Post, D. G. (2002). Against’against cyberanarchy’. *Berkeley Technology Law Journal*, 17, 1365–1387.

Reinicke, W. H. (1999). The other world wide web: global public policy networks. *Foreign Policy*, 117, 44–57.

Slaughter, A.-M. (2009). *A new world order*. New Jersey: Princeton University Press.

Shirky, Clay (2009), *Here Comes Everybody. The power of organizing without organisations*, Penguin Books.

Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, 63(3), 382–412.

Trachtman, J. P. (1998). Cyberspace, sovereignty, jurisdiction, and moder- nism. *Indiana Journal of Global Legal Studies*, 5(2), 561–581.

Verdelho, P., Bravo, R., & Lopes Rocha, M. (2003). *As Leis do Cibercrime*, volume I. Lisboa: Centro Atlântico.