Francesco Amoretti. Associate Professor of Political Science and of E-democracy and E-Government Policies at the Università degli Studi di Salerno, Dipartimento di Scienze politiche, sociali e della comunicazione. His recent research activity, basically developed within the general field of relationship between media and political systems, regarded three areas which can be described as: Mediatization of politics in Italy; the Electronic Government, and the digital revolution and the processes of constitutionalisation.
Contact: amoretti@unisa.it

Mauro Santaniello. Mauro Santaniello is a researcher at the Dipartimento di Scienze politiche, sociali e della comunicazione of the Università degli Studi di Saleno. His research focuses on Internet regulation and on the relationship between digital networks and power.
Contact: msantaniello@unisa.it

GOVERNING BY INTERNET ARCHITECTURE

Francesco Amoretti
Università degli Studi di Salerno

Mauro Santaniello
Università degli Studi di Salerno

Reception date 3th April 2014; acceptance date 30th April 2014. This article is the result of research activities held at the Dipartimento di Scienze politiche, sociali e della comunicazione (Università degli Studi di Salerno).

Abstract

In the past thirty years, the exponential rise in the number of Internet users around the word and the *intensive* use of the digital networks have brought to light crucial political issues. Internet is now the *object* of regulations. Namely, it is a policy domain. Yet, its own architecture represents a new regulative structure, one deeply affecting politics and everyday life. This article considers some of the main transformations of the Internet induced by privatization and militarization processes, as well as their consequences on societies and human beings.

Keywords

Cyberpower, Internet governance, Internet regulation, network design, digital rights

Resumen

En los últimos treinta años ha crecido de manera exponencial el número de usuarios de Internet alrededor del mundo y el uso intensivo de conexiones digitales ha traído a la luz cuestiones políticas cruciales. Internet es ahora objeto de regulaciones. Es decir, es un ámbito de la política. Aún su propia arquitectura representa una nueva estructura

reguladora, que afecta profundamente la política y la vida cotidiana. Este artículo considera algunas de las principales transformaciones de Internet inducida por procesos de privatización y militarización, como también sus consecuencias en las sociedades y en los seres humanos.

Palabras clave

Ciberpoder, gobernanza de Internet, regulación de Internet, redes de diseño, derechos digitales

Introduction

According to *Internet Live Stats*, Internet users are currently 2.9 billion. Today, around 40% of the world population has Internet connection. In 1995, this was less than 1%. During the last ten years, Internet population has been growing at an average rate around 350%, though such an increase has not been even throughout the world.[1] Moreover, digital networks have been adopted for all kind of social interactions. There are no transaction areas that have not been affected. In the past thirty years, the exponential rise in the number of Internet users around the word and the *intensive* use of the digital networks have brought to light momentous political issues. Of course, some of them are not entirely new: who rules the net? Through what means? How important is the Internet in *empowering people* and assisting them in claiming their basic rights? Other questions are more recent. The latter are a consequence of technological developments: has the Internet become a point of international conflict between states? Is it favouring the emergence of new institutions outside of the nation-state system? Above all, is the Internet itself a contemporary tool used to govern political processes, social relationships and human beings? As it emerges from the growing literature, Internet, as other telecommunication infrastructures in the past, is the *object* of regulations. Namely, it is a policy domain analysed from different theoretical and methodological perspectives. But, unlike other communication infrastructures, the Internet architecture is itself a new regulative structure affecting the political and legal order. In *Law in a digital world*, Ethan Katsh has illustrated some profound implications of technological innovations for the legal practice and the nature of the law.[2]

1. http://www.internetlivestats.com/internet-users/
2. E. Katsh, *Law in a Digital World*, Oxford University Press, Oxford, 1995.

However, between the 1980s and the mid-1990s, the dominant concern was to verify the resilience of democracies in the face of the challenges posed by technological change. How, in other words, the existing constitutional order could absorb – and govern – such transformations. In the end, thanks to normative-regulatory practices developed over the past two centuries, democracy seemed capable of coping with it, all in preserving the core values of the American liberal tradition.

At the beginning, the expectations and norms created by the Internet were radically *liberal* in nature, and gave new vitality to ideals of freedom of expression in politics and society, and to concepts of freedom of exchange and open, competitive access to information and communication markets in the economic sphere.[3]

Legitimized by this ideological-cultural milieu, the notion that the state should keep at a distance from processes of technological change was, in those years, the focus of two major initiatives that also became the reference point for the political and intellectual debate, not only in United States but also elsewhere. The first, in 1994, was the establishment of the Progress and Freedom Foundation (PFF) to which we owe the *Cyberspace and the American Dream: A Magna Charta for the Knowledge Age*. Two years later, at Davos, Perry Barlow launched *A Declaration of Independence of Cyberspace*. In their most significant passages, the two documents foreshadowed a world, the cyberspace, where governments could exercise any form of sovereignty. A free world ensuring freedom for all. Blurred in the off-line world, the dream of the Founding Fathers could thus live on in the virtual world. The state does not leave the scene. But the scene it now inhabits is the one that, because of its characteristics, escapes its control.[4] To this "borderless and timeless world" is offered an extraordinary power, that of resetting history on radically new bases. A myth, however, destined to crumble in a very short time.[5]

As virtual reality increasingly comes to resemble the real world, Cyberspace simply becomes another arena for the ongoing struggle for wealth, power and political influence: "The Net has lost its political innocence."[6] Internet, therefore, increasingly seems a space perfectly regulated and controlled, a space where the sovereignty of states and the power of ICTS corporations can be exerted. In other words those institutions that are contested and/or rejected by the libertarian and egalitarian ideologies of cyberculture,

3. L. M. Mueller, *Networks and States: The Global Politics of Internet Governance*, The MIT Press, Cambridge (Mass.), 2010.
4. J. R. Davis – D.G. Post, "Law and Borders: The Rise of Law in Cyberspace", in *Stanford Law Review*, vol. 48, 1996.
5. V. Mosco, *The Digital Sublime: Myth, Power, and Cyberspac*e, The MIT Press, Cambridge (Mass.), 2004.
6. D. Resnick, "Politics on the Internet: The Normalization of Cyberspace", in Ch. Toulose, T.W. Luke (eds.), *The Politics of Cyberspace*, Routledge, New York-London, pp. 51-54.

are the real protagonists of the struggle for control over the network, a struggle that has now gained a global scope.

Already a few years before 9/11, with the increasing public and academic attention over these issues, the notion emerged that politics are not external to the technical architecture. As a site of control over technology, the decisions embedded within it contribute to shape values, reflecting socioeconomic and political interests. We can consider this trend to be a fundamental shift in strategy, from regulating the use of technology through law to regulating the design of technology in order to control its use.

Policies – and the technical choices – that act on the architecture of cyberspace (co)-determine the kind of society we build. Since they express values and principles that, shaping the architecture of the Net, govern our behavior, they represent policies and decisions of constitutional significance. A point of no return in contemporary political and legal thought: "Code is law" is the famous formula coined by Lawrence Lessig to describe the ways in which the technological architecture of the Internet functions as a regulator – in addition to state law, social norms and the market.[7] The technological architecture of the network imposes rules on access and use of information. Technological architectures may prohibit certain actions on the network. Technology may also offer policymakers a choice of information flow rules through a configuration of decisions. The technological architecture is a structure that conditions regulation over the Internet. Hence, the code does not directly regulate the Internet, but rather prestructures the form that regulations over the Internet may take on in order to be effective in conditioning social behaviour.[8] The increasing awareness that decisions made during technological architectures design – hardware and software, protocols and standards – have significant political and public policy consequences, explains the attempts to place the Internet under closer control. I t also sheds light on the complex geopolitical dynamics arising from it. If debates – and the decisions – over technological architectures are a continuation of *politics by other means*, then the efforts to control and define such technological devices are the real issues at stake. Yet even as an Internet-enabled world challenges the state as the preeminent institution for the production of communication and information policy, it also generates strenuous reassertions of national authority.[9] These issues bring us to the nation-states system and

7. L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.
8. B. C. Graber, "Internet Creativity, Communicative Freedom and a Constitutional Right Theory Response to 'Code is Law'", in S.A. Pager, A. Candeub (eds.), *Transnational Culture in the Internet Age*, Edward Elgar, Cheltenham (UK) , 2012.
9. See, for example, J. Goldsmith, T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, New York, 2006.

to the relationship between national sovereignties and the new institutions of global governance that try to define distinct "roles and responsibilities" for governments, businesses, and civil societies. "The question now driving discussions about Internet politics is not whether the Net can be governed, but whether there is (or should be) something new and different about the way we do so."[10] Today, the new issue at stake is the de-Americanization of the Internet. Indeed, this means, rather paradoxically, going back to the fathers of the Internet. As we can read on the home page of the *Net Mundial–Global Multistakeholder Meeting on the Future of Internet Governance* (Sao Paolo, Brazil, 23/24 April 2014): "When the fathers of the internet came up with the world wide web, they conceived a web architecture which is free and open. Therefore, as the world meets in Brazil to discuss the future of the internet it must bear in mind this facts and reflect upon the visions of the founders." Has the future an ancient heart? Rather surprisingly, to properly grasp the issues at stake, it might be useful to describe that history, its driving forces and ideas, and then, move on to analyse recent developments of the Internet.

The Origins of Network Regulation: The *ad hoc* Governance Regime

In 1969 the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense achieved the interconnection of computers deployed in distant places on US territory. ARPANET was the first computer network based on the principle of packet switching, a transmission technique through which a message is divided in multiple packets that follow different paths to reach their destination, where they are then reassembled. This principle was designed by Paul Baran in order to overcome the risk that a Soviet missile attack might destroy the US military communication infrastructure.[11] The launch of the Sputnik in 1957 and the 1962 Cuban missile crisis solicited Baran's research at the RAND Corporation, a Pentagon contractor specialized in strategic analysis and research on warfare. The core idea of Baran's network was 'decentralization'. As Manuel Castells points out, Baran's design inspired a communications architecture based on three principles: decentralized network structure; distributed computing power throughout the nodes of the network; redundancy of functions in the network to minimize the risk of disconnection.[12]

10. L. M. Mueller, *Networks and States*, p. 1.
11. P. Baran, "On Distributed Communications: Twelve Volumes", in *RAND Report Series*, 1964.
12. M. Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford, 2001, p. 17.

To keep complexity management at the end point of the network meant subverting the concept of the 'terminal' itself, breaking the dichotomy master/servant, fragmenting the mainframe in a computing-power-sharing galaxy. It was an idea influenced by J. C. R. Licklider,[13] head of the Information Processing Techniques Office (IPTO) at ARPA, the same office that was financing, at that time, Baran's research at RAND. The idea of an open decentralized network was also influenced by another contemporary computer scientist, Leonard Kleinrock,[14] who was then a professor at UCLA, working on packet networks and influencing key personalities like Vint Cerf, Steve Crocker and Jon Postel. On 22 November 1977, taking advantages of the decentralized structure of ARPANET, these scholars were able to interconnect different networks with a common open protocol. Decentralization of the key functions of networks was a principle that oriented other designs of the early Net. For example, the end-to-end argument set forth in 1981 by H. Saltzer, David P. Reed and David D. Clark contended that in a communication network it is important to keep as many operations as possible at the extremities, avoiding locating protocol functions within the transmission infrastructure.[15] Decentralization also inspired David Eisenberg's glorification of "the stupid network", that is, a network that, like the Internet, locates all the intelligence at the network's periphery, keeping the middle infrastructure 'stupid'.[16] A network that differs from telephones networks that have computers in the centre of the infrastructure in order to address calls, to check credit and permissions, to apply fees. There was a common belief that Internet infrastructure should be just moving bits from point A to point B. All operations should be done by the user device. Another principle, based on this idea of decentralization, is network neutrality. In a nutshell, this principle prescribes handling all data as if it were of equal importance. According to such notion, the infrastructure should not consider the nature of packets, should not manage or even gather data, and should not discriminate between connections and content.[17] Wherever a message goes to and comes from and whatever it means, it should always be delivered as others, on a first-come first-served principle.

13. J. C. R. Licklider, "Man-computer Symbiosis", in *IRE Transactions on Human Factors in Electronics*, vol. 11, 1960, pp. 4-11. See also J. C. R. Licklider-W.E. Clark, "On-line Man-computer Communication", in *Proceeding AIEE-IRE '62 Spring Joint Computer Conference*, ACM, New York, 1962, pp. 113-128.
14. L. Kleinrock, "Information Flow in Large Communication Nets", in *RLE Quarterly Progress Report*, 1961.
15. H. Saltzer – D.P. Reed – D. D. Clark "End-to-End Arguments in System Design", in *ACM Transactions on Computer Systems*, vol. 2, no. 4, November 1984, pp. 2772-2788. Online at: http://web.mit.edu/saltzer/www/publications/endtoend/endtoend.pdf. An earlier version appeared in the Second International Conference on Distributed Computing Systems, April, 1981, pp. 509-512.
16. D. S. Isenberg, "The Rise of the Stupid Network", in *Computer Telephony*, August 1997, pp. 16-26.
17. T. Wu, "Network Neutrality, Broadband Discrimination", in *Journal of Telecommunications and High Technology Law*, vol. 2, 2003, p. 141.

Decentralization of computing power, openness of protocols, redundancy of connections, all of these principles formed a set of common beliefs about networks, their scope and their architectural structure. All this implied the autonomy of each node of the Net, a principle that turned a warfare technique into a wider political philosophy. These principles, later formalized by David D. Clarke in 1988,[18] and by Brian Carpenter in 1996,[19] had already been shaping informal guidelines for every decision and action for decades. They were shared believes; a widely accepted set of design values so commonly felt that there was no need for enforcement. They were observed not in force of a declaration – which, in some cases, were published when the principles were no longer in use – but in observance of a common vision of the Internet as a decentralized and open network. An important aspect that influenced this 'open' philosophy was the fact that, for the first fifteen years, ARPANET was developed and used only by a limited circle of American researchers. As Malte Ziewitz and Ian Brown point out:

> given the rather small and close-knit group of engineers and academics who were involved in the early Internet, coordination and control took largely place on an interpersonal basis wherever a problem was identified. Problems were conceptualized as mostly 'technical' ones, which just needed to be 'engineered' with the tools and approaches people used in their day-to-day professional work.[20]

The common framework of values, visions and beliefs, the cultural homogeneity of a small circle of Anglo-Saxon engineers and the technical nature of the problems they were facing at the time, produced a horizontal problem-solving approach to network regulation. It was a regime that Castells has called "ad hoc governance."[21] In this social, technical and cultural contest, the issue of network regulation was not perceived as a problem. Decisions on technical issues were made on the basis of what was later called "rough consensus and running code",[22] an informal decision-making process based on the dominant view of a working group interested in finding practical solutions that could be swiftly implemented.[23] The process typically started with a *Request for*

18. D. Clark, "The Design Philosophy of the DARPA Internet Protocols", in *Computer Communication Review*, vol. 18, n. 4, August 1988, pp. 106–114.
19. B. Carpenter, "Architectural Principles of the Internet", in *Request for Comments*, 1958, IAB, June 1996.
20. M. Ziewitz–I. Brown, "A Prehistory of Internet Governance", in I. Brown (ed.), *Research Handbook on Governance of the Internet*, Edward Elgar, Cheltenham, 2013.
21. M. Castells, *The Internet Galaxy*, p. 31.
22. D. Clark, "A Cloudy Crystal Ball – Visions of the Future", in *Proceedings of the Twenty-Fourth Internet Engineering Task Force*, Massachussets Institute of Technology, NEARnet, Cambridge, July 13-17, p. 543.
23. S. Bradner, "IETF Working Group Guidelines and Procedures", in *Request for Comments,* 2418, September, 1998.

Comments (RFC), a document describing ideas and innovations submitted to the research community for peer review.[24] During the first stage of the network's history, Internet developers and users were living in academic communities, and were used to reach decisions through written, argued and rational discussions. It was a situation that changed with the popularization of computer networks.

Popularization has its origins in some of the great innovations occurred in the 1980s: the Internet and the personal computer. Internet was born through the transformation of ARPANET from a network developed and used by US military, academic and industry researchers into an open international network for civil and commercial purposes. This transformation was strongly affected by two main decisions taken by ARPA in 1983: the split of ARPANET into two separate networks – Internet for civil use and Milnet for military communications – and the release of the Internet Protocol Suite (IPS), an open set of standards for networks interconnections. The giving up of the Net by the army bestowed on a few researchers working on projects funded by the US government the task of managing the Internet. They soon organized themselves and gradually gave life to the so-called native institutions of the Internet. Examples of these institutions are the Internet Engineering Task Force (IETF), an open organization based on a free participation of whoever was interested in expressing an opinion on technical issues, and the Internet Assigned Numbers Authority (IANA), working under the moral authority of Jon Postel at the Information Sciences Institute of the University of Southern California. Postel played a fundamental role in the managing of those few centralized resources that the growing net required during the 1980s. He administered the so-called root zone, a set of servers where the correspondences between names, such as *ucla.edu*, and numbers, like *128.97.27.37*, were stored. His addressing system worked according to the Domain Name System (DNS), an open network protocol designed to manage this critical resource.

Even the IPS protocols–the Internet Protocol (IP) and the Transmission Control Protocol (TCP) – were open. Every network could use them without requiring permission. They were focused on simply exchanging data in a network, addressing messages (IP's function) on the cheapest available route (TCP's job). ARPA's decisions fostered the adoption of the IPS by a growing number of other networks that were being set up by research centres across the world. The focus on civil purposes and the openness of

24. RFC was invented by Steve Crocker very early in the history of the Net – indeed, in the same year of the first connection – and later became the official working procedure of the Internet Engineering Task Force (IETF) and the Internet Society (ISOC).

basic protocols led to the creation of an international network integrating more and more local networks.[25]

The second innovation that contributed to creating the conditions for an Internet for the masses was the launch of the first personal computer by Apple, the Macintosh. By introducing *Graphic User Interfaces* (GUIs) and ergonomic interfaces such as the *mouse*, Apple opened the computer world to the wider public. Macintosh PCs were cheap, small and easy to use compared to the standards of the time, when computing was a deal of the so called mainframes: expensive and big computers requiring well-trained users. Apple launched its first personal computer in 1984, announcing it during the Superbowl with a video commercial directed by Ridley Scott. The payoff of this TV commercial was: "On January 24th, Apple Computer will introduce Macintosh. And you'll see why 1984 won't be like '1984'". Reference was to George Orwell's masterpiece and to his dystopian vision of a Big Brother watching everything and manipulating people's consciences. Giving the masses the opportunity to process information with a computer in the same way that big organizations did, Apple promised to avoid the insurgence of 'all-knowing' centres. Interfacing represented another mile-stone innovation of the Net. In the early 1990s Tim Berners-Lee, a researcher at the Conseil Européen pour la Recherche Nucléaire (CERN), invented the World Wide Web (www), a set of standards capable of graphically representing information available in the Internet. Interfaces, after having put in to communication man and machine, linked the man to the Internet. Later, in the 2000s, interfaces were also deployed on servers' administration functions. The so-called Web 2.0 allowed people with a low technical expertise to publish content on the net and to administer complex functions on a hosting server.

Interfacing is a process based on delegation. Instead of commanding the machine through its own language, users interact with it through a set of pre-packaged actions, already conceptually gathered, graphically represented and translated into instructions for computers. These instructions are in the source code of the program. When the program is running, its source code produces a representation of available actions to the user, gathers human feedback, and sends commands to the machine. The source code instructs a computer on what to do, and when and how to do it. As Lawrence Lessig pointed out, "code is law in cyberspace."[26] With interfaces users delegate to programs, and to those who have written them, the control over their own computer, their browsers

25. P. Weiser, "Standards and the Internet", excerpt in P. Weiser, *Internet Governance, Standard Setting and Self-Regulation,* 28 N. Ky. L. Rev. 822, 2001.
26. L. Lessig, *Code and Other Laws of Cyberspace*.

and their web space. Initially, the source code was 'open', instructions were known, and it was possible to read and manipulate the rules. Code creation and the modification of codes produced by others were not limited in any form. Things, however, soon changed.

Even if inspired by notions of openness and decentralization, the birth of the Internet and the launch of personal computers provided the conditions for important transformations that in the 1990s radically changed the political characteristics of digital networks. And they did it in a way that hindered the decentralized structure of the early Net.

The Privatization of the Net Regulation: The Rise of Internet Governance

During the 1990s, networks and computers underwent important changes. IETF flowed into the more organized and institutionalized Internet Society (ISOC), and IANA into the Internet Corporation for Assigned Names and Numbers (ICANN). Jon Postel was ousted by DNS management and lost his battle against the privatization of the DNS root zone. The National Telecommunications and Information Administration (NTIA), an agency of the United States Department of Commerce, took on the authority over the DNS root zone, while its ordinary management was assigned to a private company. The High Performance Computing Act of 1991 (HPCA), in order "to ensure continued United States leadership in high-performance computing", deployed huge public investments in supporting software and hardware innovations, as well as for the creation of high-speed fibre optic networks.[27] The Act strengthened the alliance between the government, the industry and the university in the United States, and accelerated deregulation and privatization processes in the telecommunications sector. In 1996 President Bill Clinton signed the Telecommunications Act, which finally deregulated the media market in the USA and gave the opportunity to companies operating in a given sector (such as broadcasting) to enter other ones (for example the telecommunications or software sector). Presented as an impulse to the improvement of market competition, the Act was to be a strong force in fostering inter-sectorial acquisitions and merging between information giants. On 1 January 1998 the World Trade Organization's (WTO) Agreement on Basic Telecommunications Services was implemented, compelling OECD nations to liberalize

27. L. Kleinrock, "The Internet Rules of Engagement: Then and Now", in *Technology in Society*, 26 (2–3), April–August 2004, pp. 193–207.

their telecommunication market and to open it to international market competition.[28] The USA and the UK had been read for this, as AT&T monopoly was dismantled on 1 January 1984 and in that same year British Telecom was privatized.[29] A private managed infrastructure eroded the openness of the protocols as it produced an unequal network. There were in fact zones interconnected by broadband connections, typically in the United States, and zones depending on marginal nodes with narrow bandwidths. Upon this unequal infrastructure, a technically neutral protocol such as the TCP, one that enabled messages to be directed towards the less overcrowded paths, had a deep political impact. Since the USA had the greatest worldwide bandwidth capacity, thanks to its cable high-speed networks it began attracting the worldwide Internet traffic towards its own territory, to its own infrastructure. It was easier that packets sent from Europe to Russia or from Africa to China passed through American servers then taking the route a plane would have. Moreover, thanks to deregulation policies a hierarchy emerged between networks. Some Internet Service Providers (ISP), precisely nine organizations, joined by means of redundant cable connections with a very high speed, forming the Tier 1 Network, the backbone of the Internet. Other ISPs were directly connected only to some nodes of the backbone (T2) and in turn provided connection to many others ISPs on a local level (T3).

Privatization occurred also as regards Internet content. In order to enforce copyright, violent dramatic battles were fought by the industry backed by the state powers: legislators, governments and courts. Industry-led architectural changes and a vast number of laws, policies, and verdicts showed that the Internet was no longer the free encyclopaedia of the human culture. Content was a property, and property, in the capitalist world-system, had to be protected. The cornerstone of the global legal system set to defend intellectual property rights lay in a couple of treaties signed in 1996 at the World Intellectual Property Organization (WIPO): The World Copyright Treaty (WCT) and the Performances and Phonograms Treaty (WPPT). These treaties introduced the concept of "electronic rights management information", that is, "information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work."[30] Conditions of use were thus enforced by this information encoded in the digital work itself. Digital products or devices were officially delegated to apply limitations to users. If a movie was sold, for example, for just a single vision or for multiple visions but only on the same device, this

28. P. Cowhey – M. Klimenko, "The WTO Agreement and Telecommunications Policy Reform", in *Policy*, Research working paper, no. WPS 2601, 2001.
29. A. Mattelart, *Histoire de la société de l'information*, Editions La Découverte, Paris, 2001.
30. Art. 12 of WCT.

private agreement could be directly enforced through this information management. WIPO treaties legitimized the principle that the source codes of digital products could also encode political instructions that do not concern only functional operations, but that also pertain to users' behaviours. The treaties committed signatory nations to protect these regulating codes providing "adequate and effective legal remedies against any person acting to remove or alter electronic rights management information without authority." WCT and WPPT were adopted by many nations, and in the USA they gave birth to the 1998 Digital Millennium Copyright Act. Even the source code of software was privatized. As we have seen before, interfaces are produced by the instructions of the source code. These instructions act as intermediaries in the man-network interplay, stating what computers must do and when and how they should do it. We have seen that the source codes of the early net were generally 'open', in the sense that it was possible to read and write over them. But during the 1990s a particular political kind of code on mass computers started being used. It was called proprietary source code. It is offered on the basis of a right to use license, within a private commercial relationship, typically between an American corporation and a user. It is protected by copyright laws and by technical barriers, so that it is not possible to read what it instructs a 'personal' computer to do. Under the private laws of Intel, Microsoft, Adobe, Google and other software companies, mass codes became secret laws, private regulators, *arcana imperii*. In this private environment, corporations became coding authorities,[31] creating a blurry private regime of public powers.[32] Simple interfaces produced, on the one hand, the growth of Internet users and of content; and on the other hand, a growing power within a new circle of intermediaries such as software houses, service providers and hardware manufacturers. Given this condition, even if the computing capacity came to be decentralized in a myriad of small computers diffused in every house, office and school, the power to determine what the computing capacity is used for – let us say computing power – was once again concentrated in a few centres on the East Coast.[33] Due to the privatization of the source code, the introduction of interfaces between man and machine, welcomed as a liberating technology, at the end bestowed an enormous power onto a few subjects able to encode within mass software whatever instruction they willed. Apple's promise to horizontally distribute power among the people turned out

31. L. Lessig, *Code and Other Laws of Cyberspace*.
32. G. Teubner, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Armando Editore, Roma, 2005.
33. M. Santaniello, "Diritti umani nel ciberspazio. Patrimonio, persona e lex digitalis", in *Politica del Diritto, (Diritti e sfera pubblica nell'era digitale)*, XLI, 3, 2010, pp. 419-440.

to be a lie. Paradoxically, Steve Jobs' company became one of most tenacious producers of proprietary source codes, and a pioneer of so-called Internet Appliances, that is, devices architecturally closed, remotely controlled and less generative than computers.[34] With its iPod and iPhone, and later with the iPad, Apple repudiated the decentralizing philosophy of its origins, and heavily reduced the computing autonomy of its users.

Privatization of Internet infrastructure, content and code reduced the scope of the first architectural principles of the net, namely, its decentralized structure, its openness, the redundancy of functions, the distribution of computing power throughout the nodes. Some nodes became more important and powerful than others. But, notwithstanding these transformations and in spite of their political consequences, throughout the 1990s and 2000s the mainstream debate on Internet regulation continued to be framed within a non-conflicting framework. More precisely, within the framework of Internet Governance (IG). The main object of regulation, in this framework, was the user's own behaviour. The actions of states, corporations and government, on the contrary, were almost ignored. As demonstrated by Ian Brown, Western institutions acted more promptly in proposing new measures against deviant users' behaviour – like file sharing, pedo-pornography and terrorist propaganda – than in ensuring the protection of fundamental rights in the information age.[35] In a map created for the Working Group on Internet Governance (WGIG) by two of the most influential research centres of legal knowledge on networks, the policy field of IG is limited to issues such as digital copyright, domain names, cybercrime, e-contracting, dispute resolution, foreign commercial relations, relations between private parties, taxation, e-banking, e-finance, jurisdiction.[36] These are all issues concerning property rights and their defence against Internet users. The only issue concerning human rights that was addressed was privacy. But in the liberal perspective adopted by the IG, privacy had been treated more as a property right (the personal property of one's own data) than as a non-fungible personal right (such as dignity, reputation and honour). The WGIG itself gave a controversial report for the World Summit on the Information Society (WSIS) that took place in 2005 in Tunis.[37] Essentially, the report proposed a working definition of Internet governance; it assigned roles and responsibilities to governments, the private sector, and civil society; and delineated a multi-stakeholder approach to decision making processes. Moreover,

34. J. Zittrain, *The Future of the Internet And How to Stop It,* Yale University Press, New Haven & London, 2008.
35. I. Brown, "Internet Self-regulation and Fundamental Rights", in *Index on Censorship*, 39 (1), 2010, pp. 98-106.
36. NetDialogue, "Clearing the House on International Internet Governance", Harvard Law School's Berkman Center for Internet and Society, 2005. At: https://web.archive.org/web/20091001015044/http://www.netdialogue.org
37. WGIG, *Report of the Working Group on Internet Governance,* 2005, http://www.wgig.org/docs/WGIGREPORT.pdf, p. 6.

it established four key public policy areas of Internet governance, mirroring the map of Harvard's Berkman Center and Stanford's CIS.

This part of the report, which focused on users' regulation, network security, and on some intergovernmental disputes over critical centralized resources, was recognized in the official Tunis Agenda for the Information Society.[38] Instead, another part of the report, more critical on some important political issues, left no trace in the final document. In this part WGIG had addressed controversial issues such as the "unilateral control by the United States Government" on the root zone files and system, the "uneven distribution of interconnection costs" from which ensued that "countries remote from Internet backbones must pay the full cost of the international circuits"; the "barriers to multi-stakeholder participation in governance mechanisms". The last issue is particularly important. The WGIG explained that:

> a) there is often a lack of transparency, openness and participatory processes; b) participation in some intergovernmental organizations and other international organizations is often limited and expensive, especially for developing countries, indigenous peoples, civil society organizations, and small and medium-sized enterprises (SMEs); c) the content produced by some intergovernmental organizations and other international organizations is often restricted to members only or is available at a prohibitive cost; d) frequency and location of venues for global policy meetings causes some stakeholders from more remote areas to limit their participation; e) there is a lack of a global mechanism for participation by Governments, especially from developing countries, in addressing multisectoral issues related to global Internet policy development.[39]

All of these matters were not properly addressed by the Tunis Agenda and the final document also avoided addressing the requests from emerging countries to move the control over DNS and other critical resources from ICANN to a UN agency. On the contrary, it called for another summit ten years from then. This demonstrated that the multi-stakeholder governance model, which postulates a free participation of different actors in defining the way digital networks were governed, turned to be serving, essentially, as a discourse platform between the American government and private stakeholders. A number of other world forums, international workgroups and

38. WSIS, *WSIS-05/TUNIS/DOC/6(Rev. 1)-E*, 18 November 2005, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html
39. See note 38, p. 6.

organizations were conceived to give all stakeholders the opportunity to express their visions about Internet regulation. But no political representation was assured to the interconnected masses and, under the flag of self-regulation, no normative power was given to any really democratic organization. The multi-stakeholder governance model legitimized the privatization of the Internet regulation, hiding it under the cloak of an open form of participation. The discourse about political power was kept at the margins of the IG debate, and the idea that a technical and administrative governance of the Internet was sufficient to regulate digital networks became dominant. The de-politicization of Internet regulation fostered by the IG paradigm was often supported by argumentations reflecting the libertarian design principles of the early Net. Even if, as we have seen, those principles had been gradually narrowed down by the privatization of the Internet, Internet was still assumed to be a decentralized system of equivalent nodes,[40] managed by a transnational multi-stakeholder partnership, drawing together a plethora of technical authorities with shared responsibilities.[41] The discourse about openness and decentralization became, from a normative informal belief, a mystifying formal representation hiding a completely altered empirical reality. A reality made of an architecture oriented more to security and property defence than to the freedom and autonomy of each node.

The Re-militarization of Networks: Cyber-power and the Internet of the Bodies

The great mystification ended in 2013. On 6 June *The Guardian* published the first of a long series of revelations about how the US government in using the Internet for its mass surveillance programs, collecting, storing and processing billions of human interactions, in America as well as everywhere else in the world. Together with their British colleagues working at the Government Communications Headquarters (GCHQ), the National Security Agency (NSA) was caught using the re-centralized, opaque and secured architecture of the Internet, built during the 1990s by corporations, in order to know everything about everyone. Documents leaked out by the whistle-blower Edward Snowden showed that Anglo-Saxon governments were downloading, on daily basis,

40. S. E. Gillet–M. Kapor, "The Self-governing Internet: Coordination by Design" in B. Kahin, J. Keller (eds.), *Coordination of Internet*, The MIT Press, Cambridge (Mass.), 1996.
41. N. Desai, "Foreward", in W. Keinwachter (ed.), *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment*, Marketing fur Deutschland GmBH, Berlin, 2007.

billions of emails, social network activities, phone and VoIP calls, video conferencing, streaming transmissions, web click stream, bank account operations, file transfers and stored data. They were doing this throughout PRISM, a secret program collecting information from databases of American information corporations like Microsoft, Google, Yahoo!, Facebook, YouTube, Skype, Aol, Dropbox and Apple. Moreover, they were taking advantage of the TCP effect – which, as we have shown, consists in attracting the world Internet traffic on to the American information superhighways – in order to store, process and analyse a great amount of global traffic. They were also taping into submarine international fibre-optic cables to access global communications; they were targeting foreign countries leaders and persons of interest through spying activities and intercepting webcams with the Optic Nerve program. Documents published by *The Guardian* revealed that NSA was infiltrating thousands of computer systems of citizens, organizations, companies and enemy countries. They were even paying tech companies to insert weaknesses into products and they were able to undermine Internet security by planting vulnerabilities in encryption standards like the one adopted in 2006 by the National Institute of Standards and Technology (NIST) and later by the International Organization for Standardization (ISO), which counts 163 countries as members.

Electronic espionage was not a novelty in international relations, nor was government surveillance of electronic communications unknown. Concerns about American agencies surveillance programs had already been expressed by several organizations at all levels. In 1999, for example, the European Parliament addressed the issue of the American electronic espionage system codenamed Echelon.[42] In 2003 the DARPA's Total Information Awareness, a project gathering an enormous amount of data, was defunded by Congress after public criticism–though it simply changed name into Terrorism Information Awareness. But the 9/11 attack limited disapproval and criticism towards US security policies and, abroad, the War on Terror prepared Western countries to be more tolerant towards US secret activities. One month and a half after the attack, President George W. Bush signed the Patriot Act. It drastically curtailed civil rights of Internet users inside and outside American jurisdiction, while expanding technical and legal possibilities for secret actions. Some provisions of the Act were lately declared unconstitutional, but the main body of the law was reauthorized by three bills until 2010. On 26 May 2011 President Barack Obama signed a further four-year extension of some of the Act's key provisions, extending surveillance permissions on devices and data.

42. STOA, *Development of Surveillance Technology and Risk of Abuse of Economic Information*, PE 168.184/Vol 5/5, 1999.

As the mix of architectural and legal changes allowed the privatization of the Internet in the 1990s, by 2001 the same mix worked to get the Pentagon back in control of the networks. As for users' behaviour, at the end of the first decade of the twenty-first century Internet was almost completely secured.

Power relations between states instead became more and more conflicting, above all those between the USA and China.[43] A geopolitics of the Internet begun to be drawn on maps. Low-density conflicts started to be fought through electronic armies, and silent battles were conducted mostly to steal data, infect systems and test enemies infrastructures and devices. Even if no open war was declared, governments started to face cyberwarfare, and Internet was starting to be militarized.

Between 2006 and 2013 the frequent leaks about government programs threatening civil rights and the increasing conflicting interstate relationships made critical approaches to Internet Governance less marginal than in the past–at least within the research community. The IG agenda was opened up to some thorny issues ignored for almost two decades. This opening is well testified by a 2010 paper by Laura De Nardis who, taking into account contributions by scholars focusing on power relationships in the cyberspace, expanded "the emerging field of Internet Governance" to some critical areas such as communications rights, private backbones, deep data inspection and "private industry use of trade secrecy laws to control the flow of information online."[44] But the 2013 Datagate shattered the Internet Governance. All IG's assumptions such as openness, power decentralization, rough consensus, multi-stakeholder partnership, the limitation of states power, and even the concept of governance itself went questioned. Every discourse based on trust and delegation seemed out-of-date. The empirical reality of the Internet suddenly revealed itself as an unprecedented system of always-on control erected by US governments, with a working team play between Democrats and Republicans. It was no longer surveillance. It was an automated mass surveillance. Absorbing almost entirely the "free flow of information", storing and processing it through data mining software is not just a search. It allows scanning human interactions and predicting aggregate behaviour. It allows a limited circle of people to know more than they should about other people. Moreover, surveillance is not the only goal of this system. Throughout the secured Internet, government agencies can also punish. Infiltrating a computer, damaging a communications system, hacking a protocol,

43. J. Goldsmith – T. Wu, *Who Controls the Internet?*
44. L. DeNardis, "The Emerging Field of Internet Governance", in *Yale Information Society Project Working Paper Series*, September 2010.

destroying content, software or hardware are all actions that go far beyond watching. NSA, GCHQ and other similar agencies have gained the power to take untraceable and unauthorized actions against their targets. They can control–and also command. The re-militarization of the Internet has been achieved at a critical moment of the historical process of interfacing between the man and the Net. Thanks to biometric interfaces, to mobile devices, to always-on connections, to home automation, to geo-localization facilities, to smart watches, Google Glass and other wearable technologies, the human body is getting increasingly closer to the Net. The Internet of Things is producing the Internet of Bodies, and the dream of a man-computer symbiosis expressed in a visionary 1960 article by Licklider, just before being appointed head of IPTO by the Pentagon, has almost became a reality.[45] In this scenario, with a secured network in direct touch with the human body, the issue of networked power becomes a crucial issue that urgently needs to be addressed. Ruling the Net increasingly means ruling the people, their social interactions and their own bodies. The capillary innervation of the network in the everyday material life raises serious questions about the governing systems of our time. Humanity is threatened by emerging technologies of "biopoliticized security", a security "taking the human body and its movements as the focal points."[46] These are questions that cannot be addressed with the conceptual instruments of technical governance, and that require, on the contrary, an analysis of the political government of the Net. An analysis, that is, of power itself.

Conclusions

Much research still needs to be made. Current trajectories – such as privatization, militarization processes and the escalation of conflicts – need to be investigated. They are deeply transforming the Internet and affecting human interactions in the cyberspace. What kind of cyberspace should we expect for the future? An open and decentralized 'augmented reality', or an inextricable web of snares fettering human behaviour? A shared resource for humanity, or a battlefield for cyber-powers?[47] And, furthermore, will

45. J. C. R. Licklider, "Man-computer Symbiosis", in *IRE Transactions on Human Factors in Electronics*, vol. 1, 1960, pp. 4-11.
46. A. Ceyhan, "Surveillance as Biopower", in K. Ball, K. Haggerty, D. Lyon (eds.), *Routledge Handbook of Surveillance Studies,* Routledge, London and New York, 2012, pp. 38-45.
47. M. Santaniello–F. Amoretti, "Electronic Regimes: Democracy and Geopolitical Strategies in Digital Networks", in *Policy & Internet*, 5, 2013, pp. 370-386.

power relations in the cyberspace lead to a balkanization of the Internet?[48] Are we facing a de-Americanization of global networks? What are the strategies of the most powerful actors? How do they affect human rights? Is there still a possibility of re-democratizing the Internet? Or, on the contrary, the only choice left to those who seek freedom is between diving into the Darknet, where contestation ghettoize among deviancy, and a total or a partial disconnection, an exit strategy following the example of the Russian Army that uses typewriters to keep top secret documents out of the Internet? Will the call for an *Internet Bill of Rights* be able to merge principles throughout normative standards for any actor – states, international organizations, ICT corporations and individuals? Is it still possible to *constitutionalize* the Net?[49] If the Internet does not naturally empower people, how might it do so? In order to answer these and other important questions – all of which will have a deep impact on the political nature of human societies in the ensuing years – it is necessary to begin a wider and deeper reflection about cyber regulation. A holistic reflection that keeps constantly focused on its own research object, one that avoids ideological approached and mystifications by continuously scrutinizing its own material and technical basis.

48. K. Saunders, "Balkanizing the Internet", in S.A. Pager, A. Candeub (eds.), *Transnational Culture in the Internet Age*, Edward Elgar, Cheltenham, 2012.
49. H.L. Tribe, *The Constitution in Cyberspace. Law and Liberty Beyond the Electronic Frontier,* Harvard University Press, Cambridge, 1991.