

INTERNATIONAL LAW

QUARTERLY

www.thellQ.com



Focus on the International Aspects of Cybersecurity and Data Privacy

In this issue:

Message From the Chair.....	5
From the Editors.....	10
Access Wars: How the Second Circuit’s Opinion in <i>Microsoft v. United States</i> Changes the Rules for Government Access to Data in Cross-Border Investigations.....	12
When You Have Suffered a Data Breach, Attribution May Be Useful, But Hacking Back? Not So Much!	14
Duty Free? The Effect of International Data Privacy and Protection Laws on Employers’ Ability to Monitor Business Emails of Employees Working Outside the United States	16
Protecting Corporate Trade Secrets From Former Employee ‘Haccess’	18
The EU’s Attempt at a Comprehensive Approach to Regulation and Enforcement of Data Protection.....	20
Cybersecurity: A Sea Change in Maritime Commerce.....	22
International Legal Assistance and Special Considerations Presented in the Cybercrime Context.....	24
Internet Regulation and Data Protection: The Role of Law Enforcement	26
Homeland Security and Data Privacy: A Primer on Customs’ Global Entry Program	28
Feeling Pushed Up Against the Wall? Current U.S. Immigration Climate Demands That U.S. Employers ‘Think Outside the Box’	30
Worksite Enforcement: An Attorney’s Role in Counseling Employers About the I-9 Audit Process and E-Verify.....	32
The Bitter Side of <i>Ius Pecuniae</i> in the United States: The Risks Facing EB-5 Investors	37
The Impact of International and U.S. Domestic Law on the Future of the Global Medical Marijuana Market.....	41
World Roundup	46
Section Scene	52



International Law Section Leadership

Alvin F. Lindsay III	Chair
Eduardo Palmer	Immediate Past Chair
Arnoldo B. Lacayo	Chair-Elect
Carlos F. Osorio	Secretary
Clarissa A. Rodriguez	Treasurer
Angie Froelich	Program Administrator

International Law Quarterly

Rafael R. Ribeiro	Editor-in-Chief
Javier Peral	Editor
Loly Sosa	Editor
Susan Trainor	Copy Editor
Colleen Bellia	Graphic Designer
Clarissa A. Rodriguez	Advertising crodriguez@tenzer.com

This publication is prepared and published by The Florida Bar.

Statements or opinions or comments appearing herein are those of the editors and contributors and not of The Florida Bar or the International Law Section.

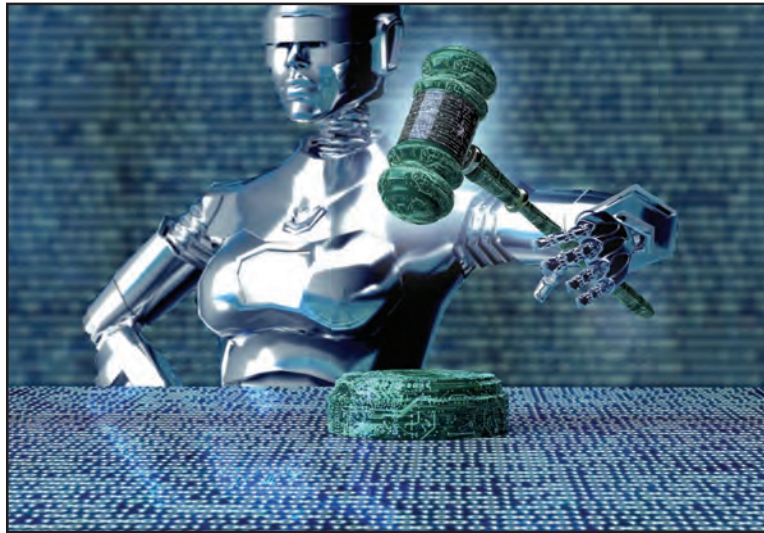
Articles may be reprinted with permission of the editor and the author(s) of the requested article(s).

Contact: Rafael Ribeiro at rafael.ribeiro@hoganlovells.com

Internet Regulation and Data Protection: The Role of Law Enforcement

By Thiago Luís Santos Sombra, Brasília

Regulation in cyberspace is becoming a myth in some parts of the world. While prohibiting software, platforms, and services like Uber, nation states are trying to deal with the disruption and convergence issue, not understanding the aim and the benefits of regulation. This essay analyzes regulation in cyberspace as the next challenge of the general theory of law enforcement.



and the physical limitations of the atomic world.³ The theoretical disputes are no longer the greatest debate about legality and morality in law.⁴ Theorization of the law throughout the twentieth century has always centered on the key themes of property and possession; this was suitable when dealing with physical

goods,⁵ but is not suitable in the realm of cyberspace when dealing with information, ideas, or the sharing economy.⁶

In the past, modern economies were structured around the ownership of material things,⁷ as highlighted by John Perry Barlow.⁸ Now the law has transitioned, due to the growth of cyberspace and its key element, information, which is not based on atoms, but on bits.⁹ Thomas Jefferson was perhaps the first man who imagined how the future could be changed by information and ideas, especially in an age when people thought only about the exclusiveness of property, as we can deduce from his letter to Isaac McPherson.¹⁰

The digitization and disruption processes that society is currently undergoing show us that nonrivalrous goods will allow us to consume, share, and produce information simultaneously,¹¹ in an unlimited manner, wherever we are and for whatever reason each person consumes it.¹² Notwithstanding the above, the law should have the ability to deal with these shifts.¹³ If information is to be our principal good and our main source of wealth—the so-called oil of the twenty-first century—then perhaps the challenges will not be in terms of ownership, but in

Regulation in Cyberspace

One of the most interesting themes encountered when undertaking research about cyberspace concerns its regulation in regard to civil society and law enforcement. One of the aims of this research is to comprehend how people's behavior in everyday life differs from their behavior in cyberspace, and what impact this difference may have on regulation.¹ This article includes a brief history of cyberlibertarianism and its decline, and then offers an explanation of cyberpaternalism and network communitarianism, two different theoretical points of view on cyberspace.

As an initial matter, regardless of which theory is most supported, it is essential to understand how intervention in cyberspace differs from regulation in real life. In this respect, a proper understanding of the particularities of cyberspace requires us to necessarily change some aspects of our conceptualization of the general theory of the law,² which has been constructed solely to resolve problems related to property, the rivalrousness of goods,

Internet Regulation and Data Protection, continued

terms of sharing information and ideas; in other words, “bits” being transferred across the globe.¹⁴

This ongoing process will represent not a change in providers, but changes regarding the services and benefits offered in society, for law cannot regulate the content itself, so it affects the recipient as Barlow has outlined with his analogy of the wine and its bottle. Law cannot affect cyberspace directly, sanctioning the actually bytes, but it can influence the physical world that supports it.

We experience numerous examples of revolutionary services, the so-called “disruptive technologies” from Uber, Airbnb, Spotify, Coursera, Netflix, VinyLify, and Prosper Marketplace all the way to SSRN-Social Science Research. Despite these variations of “bottles,” to use Barlow’s expression, it remains unclear whether the law will be successful in taming cyberspace. Why should cyberspace be regulated, who has the legitimacy to do so, who represents whom, and how will territorial limits be

drawn?¹⁵ Will sharing instead of owning change human relationships and the way the law regulates behavior? These are the key questions that this article addresses and will seek to answer.

The Cyberlibertarians and the Discovery of Cyberspace

The so-called cyberlibertarians were the first to consider the perspective of regulating rule or behavior in cyberspace. Following the creation of the World Wide Web in 1989 by Tim Berners-Lee,¹⁶ this new tool created or influenced many outcomes, which have expanded drastically over the years. Amidst this new environment, people were dazzled by the global real-time interaction it provided. Emails, chat groups, instant information sharing, and other new services quickly sparked the interest of the public, and the debate soon ignited

... continued on page 91

Sequor Law proudly salutes The Florida Bar International Law Section and its leadership among international law organizations.

You Provide a Platform for Florida’s International Practitioners to Lead Globally with Information, Innovation and Insight.

Sequor Law will continue to support your efforts as we represent clients worldwide with investigations, asset recovery and financial fraud matters, cross-border insolvencies, and commercial and financial services litigation.



SEQUOR LAW

Relentless. Global. Pursuit.
www.SequorLaw.com

Internet Regulation and Data Protection, from page 27

over how this new medium would be regulated. The prospect of online markets and unlimited information sharing quickly drew the attention of companies and governments that sought to exercise some control over cyberspace.¹⁷

In response to this first attempt at regulation, John Perry Barlow famously proclaimed the independence of cyberspace in 1996, claiming that this new environment should not be violated by state entities.¹⁸ Clearly, there was much idealism concerning the perfect equality and interaction that the network provided, where people were not affected by their physical or social aspects. Also, since the early “netizens” (so-called citizens of the Internet) were mostly techies or people who had higher computer skills, the ability to interact with this crude environment led to the illusion that the users could tailor their systems, guaranteeing free expression and liberties to all.¹⁹

The cyberspace rapidly expanded in functionalities and appliances. Newer browser interfaces, new layers, faster connections, and other features led the cyberspace to extrapolate its merely communicational purposes, and its horizon of possibilities soon demanded state intervention.²⁰ The great challenge, it seemed, was that the Internet was everywhere—today taken to the extreme of the Internet of Things—so that no particular state could properly regulate it. Regulation, however, was essential to guarantee all that the Internet could offer. In order to allow electronic commerce, the state would need to guarantee property and contract rights in the same way it did in the physical world. To hasten bureaucratic governmental processes, the state would need to guarantee that the documents circulating on the Internet could be verified in some way.

Soon, the threats also appeared. This network that brought numerous liberties also provided means of new violations. With database violations, copyright infringement, and server attacks, the companies using the Internet *needed* institutional protection in order to operate. The absence of the state would, in essence, jeopardize everything the Internet had to offer.

The bottom-up regulatory model of the cyberlibertarians soon showed its weaknesses. The global anarchy it proposed clearly would not suffice to meet the needs of interacting states, populations, and markets. In the late 1990’s, this was more than clear, and in 1996, Lawrence Lessig had already challenged Barlow’s view of cyberspace by proposing a very present state in the Internet, through his book *Code 1.0*.

Who Are the Cyberpaternalists and What Do They Believe?

After cyberlibertarians had declared cyberspace a territory of liberties, not under state control in terms of borders and sovereignty, including Barlow who proclaimed its independence,²¹ cyberpaternalists presented questions that remain unanswered.

One of those issues concerns intangible borders and regulatory procedures. For example, how can China, North Korea, and Saudi Arabia control, filter, and blacklist websites and prohibit certain software in their territory?²² Or, for instance, how is it possible for Uber to be prohibited in some clearly defined physical boundaries?²³ Also, in an attempt to propose an opposing point of view, if the cyberlibertarians are correct, how should states deal with anonymity and crimes in the deep web—named *Dot Onion/Tor*,²⁴ child pornography,²⁵ cyberbullying,²⁶ porn revenge,²⁷ cybercrimes,²⁸ data privacy violations,²⁹ disruptive services,³⁰ thefts/extortion³¹ on bank accounts, and money laundering?³² As Cass Sunstein³³ stated, it is unimaginable for cyberspace to be a democratic place without some kind of state intervention, since we do not know who represents and speaks on behalf of society.³⁴ Representation and accountability are two of the most difficult political elements of democracy, lost amidst the crowd in cyberspace.³⁵ Deliberation and decision processes in cyberspace, for example, present a new challenge in an environment where we cannot ensure that democratic values will be developed.³⁶

Cyberlibertarianism is an approach that ignores the fact that cyberspace is different from physical life, above all in its capacity to connect people who have the same

Internet Regulation and Data Protection, continued



law in cyberspace with the *lex mercatoria*, which he called *lex informatica*. For him, cyberspace was not immune to regulatory interventions; since, according to Andrew Murray,⁴¹ he identified two new regulatory borders arising from new rule-making processes involving states, the private sector, technical interests, and citizens. These components had special roles for Reidenberg and were based on contractual agreements among internet service providers (ISPs) and network architecture, becoming the new borders made and controlled by society.⁴² In sum, *lex informatica* would be the stakeholders' new model of political governance in cyberspace,⁴³ in which the regulatory process must be understood in another context, especially because legal control would be just one aspect of regulatory practice as a whole.⁴⁴

interests and to allow people to isolate themselves based on their differences. In fact, it is flagrant that governments send legal messages by regulating certain activities in order to influence the architecture of the network. France³⁷ and Australia,³⁸ for example, have just passed and upheld laws that use filtering and blacklisting controls for surveillance and for the protection of copyrights. Airbnb and Uber are changing their policies on home sharing and transport, respectively, after England and France adopted new legislation on taxed services.³⁹

The first theorist to criticize the flaws of cyberlibertarianism was Joel Reidenberg,⁴⁰ despite his agreement with Post and Johnson about imaginary boundaries and the disintegration process of territorial references. As the founder of cyberpaternalistic theory, Reidenberg established a comparison of a new rule of

Reidenberg defended the fact that principal regulatory activity would be carried out by other primary sources: technology developers and social customs.⁴⁵

Indeed, Reidenberg's position was more consistent than the cyberlibertarian's stance, particularly when he related the function of social interactions on cyberspace and the power of developers to send regulatory messages while changing the network architecture.⁴⁶ It was well noted by Reidenberg that democratic values and the "common good" are directly dependent on some kind of network control that should be provided by different actors.⁴⁷ What cyberpaternalists forgot from the start was the density and the dynamism of the multiple simultaneous interactions among stakeholders.

Conclusion

Cyberspace has spawned a new public arena of

Internet Regulation and Data Protection, continued

deliberation, and its regulation is essential to preserve democratic values and choices. Instead of mere prohibition, regulation means transforming the reality to promote the environmental conditions for the development of society. Thus, it is almost impossible to ignore society's demands for new products and services like Uber, Airbnb, and Spotify. The disruption, convergence, and digitization processes are happening with or without the state's approval, and the development of civil society will most likely be better guided if the regulation is organized conjointly between the state and individuals, instead of by cyberpaternalistic verticalism or cyberlibertarian anarchy. If the state were to limit its participation in this process by simply prohibiting or allowing innovative products and services, society would through market, social norms, and architecture overwhelm the state's legislation in order to secure the viability of cyberspace's creativity and innovation.

Cyberpaternalism ignores the huge power that non-state users have on the Internet, or even the fact that Internet culture is emerging and becoming more and more complex. This, in the end, also affects user and governmental behavior inside and outside the Internet.

States must understand that regulation can be achieved in various ways, and not just by law. Indeed, states should also act through architecture, dealing directly with the code. Obviously, such interferences must be made legitimate by the appropriate mechanisms, but the necessity for governmental presence in coding is clear. Some countries have acted by blocking and filtering lists.⁴⁸ One clear sign of this in Brazil is the city of Curitiba, the capital of the state of Paraná, which took the initiative of adapting to Internet culture by creating a Facebook page and using humorous memes and current Internet jokes to communicate messages related to public policy on health, environment, and other issues of public interest and even to increase its own legitimacy as a democratic government.⁴⁹ It is clear that there is no perfect vertical regulation exerted from the state onto its citizens, especially in the civil law countries where the legislative branch is always behind technology and

information. In fact, curiously enough, the adaptive initiative of Curitiba was noticed by citizens of other Brazilian states, thousands of miles away, and they pushed for such adaptations in their own cities.

In summary, it is safe to conclude that the Internet has led to strong readapted processes of our model of state. The Internet has multiplied drastically communicative media and information dissemination. This process has engaged in the virtuous (or vicious, depending on point of view) cycle of technical development and communication expansion. Information is flowing in unprecedented rates, quantities, and forms. This has direct impact in all aspects of society, for reasons abovementioned. In this scenario, it is essential for the state to comprehend this new reality, despite its cumbersome bureaucracy, and to adapt in order to continue to represent its citizens and properly regulate this extended environment of society. Mere binary prohibition/allowance is a failed form of regulation, and interactive presence is the only way to obtain legitimacy and effectiveness in the digital environment.



Thiago Luís Santos Sombra is a lawyer, an arbitrator, a private law professor at the University of Brasilia (UnB), a visiting researcher at the London School of Economics-LSE, a former state attorney at the Brazilian Supreme Court, and a former clerk at the Superior Court of Justice.

Endnotes

- 1 David R. Johnson & David Post, *Law and borders: the rise of law in cyberspace*, 48 *STANFORD LAW REV.* 1367 (1995).
- 2 Lawrence Lessig, *CODE VERSION 2.0 AND OTHER LAWS OF CYBERSPACE* 27 (2006).
- 3 John Perry Barlow, *The next economy of ideas: selling wine without bottles on the global net*, 8 *WIRED*, 5 (2000).
- 4 Ronald Dworkin, *TAKING RIGHTS SERIOUSLY* 76 (2008).
- 5 Jon Berkeley, *The trust machine*, *THE ECONOMIST*, 2015, <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine> (last visited 2 Nov. 2015).
- 6 Benkler, *supra* note 5 at 15.
- 7 Manuel Castells, *THE RISE OF THE NETWORK SOCIETY: THE INFORMATION AGE: ECONOMY, SOCIETY, AND CULTURE* 23 (2011).
- 8 Barlow, *supra* note 8 at 10.

Internet Regulation and Data Protection, continued

9 Andrew D. Murray, INFORMATION TECHNOLOGY LAW: THE LAW AND SOCIETY 4 (2013).

10 Thomas Jefferson, *Thomas Jefferson's letter to Isaac McPherson: Article 1, Section 8, Clause 8*. THE FOUNDERS' CONSTITUTION (1813), http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html (last visited 1 Aug. 2015).

11 Benkler, *supra* note 5 at 25.

12 Murray, *supra* note 14 at 12.

13 *Id.* at 26.

14 Barlow, *supra* note 8.

15 Andrew Murray, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 22 (2007).

16 Tim Berners-Lee, *WWW: past, present, and future*, 29 COMPUTER 69–77, 74 (1996).

17 Peter Diamandis, THESE MULTI-BILLION DOLLAR INDUSTRIES ARE RIPE FOR DISRUPTION THIS DECADE (2015), <https://www.linkedin.com/pulse/ripe-disruption-part-2-peter-diamandis> (last visited 27 Oct. 2015); Michael Rundle, *Government outlines "smartphone state," via Uber and blockchain*, WIRED UK (2015), <http://www.wired.co.uk/news/archive/2015-09/22/matt-hancock-mp-interview-digital-government> (last visited 27 Oct. 2015).

18 John Perry Barlow, *A declaration of the independence of cyberspace*, 10 WIRED (1996).

19 Gian Volpicelli & Alex Pentland: *Big data will help us hold governments accountable*, WIRED UK (2015), <http://www.wired.co.uk/news/archive/2015-10/15/alex-pentland-wired-2015> (last visited 27 Oct. 2015).

20 Benkler, *supra* note 5 at 137.

21 Barlow, *supra* note 23.

22 Murray, *supra* note 14 at 75–76.

23 Rafael Barifouse, *Mais da metade das capitais do Brasil já têm projetos de lei contra o Uber*, BBC BRASIL, 10 September 2015, http://www.bbc.com/portuguese/noticias/2015/09/150908_uber_projetos_de_lei_rb (last visited 27 Oct. 2015).

24 Andy Greenberg, *Mapping how Tor's anonymity network spread around the world*, WIRED UK, 2015, <http://www.wired.com/2015/09/mapping-tors-anonymity-network-spread-around-world/> (last visited 27 Oct. 2015).

25 The Crown Prosecution Service, INDECENT PHOTOGRAPHS OF CHILDREN: LEGAL GUIDANCE THE CROWN PROSECUTION SERVICE (1997), http://www.cps.gov.uk/legal/h_to_k/indecnt_images_of_children/ (last visited 27 Oct. 2015); Liat Clark, *Minister Joanna Shields to combat online child abuse and terrorism*, WIRED UK, 2015, <http://www.wired.co.uk/news/archive/2015-05/19/joanna-shields-new-internet-safety-minister> (last visited 27 Oct. 2015).

26 Kevin Simpson, *How a cyberbullying law in Colorado was tweaked to be more effective*, DENVER POST, 14 July 2015, http://www.denverpost.com/news/ci_28479145/cyberbullying-tweaks-colorado-law-can-impose-fines-jail (last visited 4 Aug. 2015).

27 Lizzie Dearden, *People who spread revenge porn will at last face justice*, THE INDEPENDENT, 13 April 2015, <http://www.independent.co.uk/news/uk/home-news/revenge-porn-illegal-in-england-and-wales-under-new-law-bringing-in-two-year-prison-terms-10173524.html> (last visited 27 Oct. 2015).

28 Andrea Peterson, *Could hackers take down a city?*, THE WASHINGTON POST, 18 August 2015, <https://www.washingtonpost.com/news/the-switch/wp/2015/08/18/could-hackers-take-down-a-city/> (last visited 27 Oct. 2015).

29 Abigail Tracy, *While The Supreme Court Hesitates On*

Warrantless Cell Location Data Collection, Your Privacy Remains At Risk, FORBES, 2015, <http://www.forbes.com/sites/abigailtracy/2015/10/16/while-the-supreme-court-hesitates-on-warrantless-cell-location-data-collection-your-privacy-remains-at-risk/> (last visited 27 Oct. 2015).

30 Isabela Palhares, *Celular é principal forma de acesso à internet pelos jovens - Educação*, O ESTADO DE SÃO PAULO, 28 July 2015, <http://educacao.estadao.com.br/noticias/geral,celular-e-principal-forma-de-acesso-a-internet-pelos-jovens-brasileiros,1733869> (last visited 27 Oct. 2015).

31 BBC News, FINANCE FIRMS TARGETED BY CYBER EXTORTION GANG BBC NEWS (2015), <http://www.bbc.com/news/technology-34205258> (last visited 28 Oct. 2015).

32 Greenberg, *supra* note 30.

33 Cass Sunstein, REPUBLIC.COM 2.0 25 (2 ed. 2009).

34 Volpicelli, *supra* note 24.

35 Suzanne Dovi, POLITICAL REPRESENTATION THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., Spring 2014 ed. 2014), <http://plato.stanford.edu/archives/spr2014/entries/political-representation/> (last visited 9 Oct. 2015).

36 Benkler, *Supra* Note 5 At 241; Lessig, *Supra* Note 7 At 28.

37 Jacqueline Jones, *France top court rules surveillance law constitutional*, JURIST (2015), <http://jurist.org/paperchase/2015/07/france-top-court-rules-surveillance-law-constitutional.php> (last visited 1 Aug. 2015).

38 Josh Taylor, RIGHTS HOLDERS COULD GET SITES BLOCKED WITHOUT EVIDENCE (2015), <http://www.zdnet.com/article/rights-holders-could-get-sites-blocked-without-evidence/> (last visited 4 Aug. 2015).

39 Patrick Robinson, *London reveals new policy on home sharing*, THE AIRBNB PUBLIC POLICY BLOG (2015), <http://publicpolicy.airbnb.com/london-reveals-new-policy-home-sharing/> (last visited 2 Aug. 2015).

40 Joel R. Reidenberg, *Lex Informatica: The formulation of information policy rules through technology*, 76 TEX REV 553, 554–555 (1997).

41 Murray, *supra* note 14 at 60.

42 Reidenberg, *supra* note 46 at 576–577; Andrew D. Murray, *Nodes and gravity in virtual space*, 5 LEGISPRUDENCE 195–221, 3–4 (2011).

43 Reidenberg, *supra* note 46 at 581.

44 The best examples are the statute that passed in Colorado criminalizing cyberbullying and the French HADOPI law. Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI), GRADUATED RESPONSE HADOPI LAW FOR THE RIGHTS PROTECTION HADOPI (2010), <http://www.hadopi.fr/en/haute-autorite/about-hadopi> (last visited 4 Aug. 2015); Simpson, *supra* note 32.

45 Reidenberg, *supra* note 46 at 76.

46 *Id.* at 588.; Murray, *supra* note 48 at 5.

47 Sunstein, *supra* note 39 at 32.

48 Sophie Curtis, *BT forces porn filter choice*, THE TELEGRAPH, 16 December 2013, <http://www.telegraph.co.uk/technology/internet-security/10520537/BT-forces-porn-filter-choice.html> (last visited 28 Oct. 2015); Murray, *supra* note 14 at 72.

49 Marina Pinhoni, *Curitiba é hoje cidade mais engraçada do Brasil*, Online REVISTA EXAME, 2014, <http://exame.abril.com.br/brasil/noticias/curitiba-e-hoje-cidade-mais-engracada-do-brasil-veja-razao> (last visited 28 Oct. 2015).