DE GRUYTER
OPEN

ICLR, 2017, Vol. 17, No. 1.

In the Jungle of the Unregulated: Towards Extra-Legal Regulatory Approaches in Addressing 'Cybercrime'

Artur Appazov[1]

Faculty of Law, University of Copenhagen, Denmark

artur.appazov@jur.ku.dk

APPAZOV, Artur. In the Jungle of The Unregulated: Towards Extra-Legal Regulatory Approaches in Addressing 'Cybercrime'. *International and Comparative Law Review*, 2017, vol. 17, no. 1, pp. 83–107. DOI 10.2478/iclr-2018-0003.

Summary: As the incidence and the cost of cybercrime keeps growing, the traditional legal model based on the command-and-control approach to regulation experiences major difficulties in curbing further inflation of the phenomenon. The article argues that the traditional legal approach that grounds its authority in enforcement is a poor option for regulation of online human interaction. By considering alternative avenues in influencing online behavior – community-, competition-, and design-based regulation – the article suggests reconsideration of our public policies and regulatory approaches to cybercrime. In doing so, the article offers a thorough interdisciplinary reflection on the idiosyncrasies of human interaction in network environments and its psychological implications, concluding that other regulatory powers may present more effective response to the problem of cybercrime. The holistic regulatory regime that the article advocates incorporates and coordinates all regulatory powers that exist in our societies in order to address the underlying cause of cybercrime.

Keywords: Online interactions, Cyberspace, Cybercrime, Regulatory mechanisms, Extra-Legal Regulation,

1 Introduction

The internet is celebrated for empowering the freedom of an individual to communicate, gather and share information with the rest of the world, and express oneself. To reach the global audience, both for well- or ill-intentioned activity, requires only minimum effort, whereas the indiscriminate nature of the internet empowers both constructive and deviant social behavior. The flipside of the freedom granted by the internet is known as cybercrime.

Having become an accepted term, cybercrime is more a term of the art rather than a clear and useful legal definition. Conceptually, it is a convenient marker

1 Dr. Artur Appazov (PhD Copenhagen; LLM Lund) is a Postdoctoral Fellow at the Faculty of Law of the University of Copenhagen, Denmark. He was earlier affiliated with a number of international organisations, such as the International Criminal Court, the Special Court for Sierra Leone, and most recently the United Nations Office for Project Services.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

that captures a vast array of antisocial, invasive or abusive practice that occurs by means of the information and communication technologies. Different countries treat cybercrime differently. Some of online deviance is criminalized, whereas other conduct that can be considered harmful or socially or morally wrong is not. In this article, I will use the word cybercrime as a term that refers to both the behaviour that is criminalized in various jurisdictions therefore constituting criminal offences, and non-criminalized behaviour that constitutes online conduct broadly regarded as antisocial.

Despite the legislative and the law enforcement efforts to address cybercrime, the phenomenon is only gaining pace.[2] As connectedness and communication increase all over the globe, so do various forms of cybercrime. A telling illustration of the tendency that cybercrime is nowhere near to be contained is the growth of incidence in various types of cybercrime and the costs – monetary and other – that it bears on governments, individuals and businesses. In monetary and societal terms the cost of cybercrime is immense but very few responsible are identified. In 2016, the Norton Cybersecurity Insights Report estimated the number of affected by cybercrime at 698 individuals on the planet bringing the total monetary cost to US$126 billion.[3] The number of affected people is rising by 10 percent every year turning cybercrime into an epidemic.[4] The impact is not only monetary. Online interaction has profound influence on a vast number of individuals on the planet as they depend on the internet in the private, social and business aspects of their lives. No only phones and laptops are connected to the internet these days, but home thermostats, kitchen appliances, cars, and even medical devices, to name a few. We depend on the internet in our interaction with work, friends, family, making it the main medium by which we experience the world. The number of devices connected to the Internet of Things rises every day, and by 2020 can reach the numbers six times exceeding humans on the planet.[5] Connected to the internet, all devices become potentially vulnerable. The exploitation of social networks, mobile devices and other critical technology is likely to grow.[6]

2 Symantec Corporation. *Norton Cybercrime Insights Report: Understanding Cybercrime and the Consequences of Constant Connectivity* (rep.), 2016; Symantec Corporation. *Norton Cybercrime Report: Human Impact* (rep.), 2010; RAND Corporation. *Consumer Attitudes toward Data Breach Notifications and Loss of Personal Information* (rep.), 2016; RAND Corporation. *High-Priority Information Technology Needs for Law Enforcement* (rep.), 2015; RAND Corporation. *Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar* (rep.), 2014; Hewlett Packard Enterprise. *Securing the Internet of Things* (rep.), 2015.

3 Symantec Corporation. *Norton Cybercrime Insights Report: Understanding Cybercrime and the Consequences of Constant Connectivity* (rep.), 2016, p. 5; also see Symantec Corporation. *Norton Cybercrime Report: Human Impact* (rep.), 2010.

4 *Ibid*. at 5

5 RAND Corporation. *Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar* (rep.), 2014, p. ix.

6 WELLINGTON, Katherine Booth. Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions. *Santa Clara High Technology Law Journal,*

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

RAND Corporation analysis predicts that the nearest future will be marked by greater hyper-connectivity and with it – greater darknet activity, greater anonymity and greater encryption possibilities.[7] Coupled with the stimulating monetary effect of the black market where stolen data and other vulnerabilities are sold, this will likely lead to the situation when "the ability to attack will […] outspace the ability to defend."[8] The UK Home Affairs Committee on E-Crime admitted that "[a]s the fraud and e-crime is going up, the capability of the country to address it is going down"[9] The UK is most probably not alone in this conclusion.

With the cost and occurrence of cybercrime steadily growing every year, one can conclude that neither the cybersecurity industry nor the law enforcement globally is keeping up the pace with the advances of the multi-billion dollar industry into which cybercrime has evolved. The traditional legal paradigms and models seem to be failing in addressing the rampant growth of cybercrime.

In approaching cybercrime, our current regulatory regimes in their strategies and policies seem to be fixated on the command-and-control approaches, effectively disregarding the utility of such community-based forms of regulation, as social norms and the market, as well as of technological regulation.[10] The traditional command-and-control regulation that mandates certain conduct through a piece of legislation seems to conceptualize the internet and everything that happens in it as yet another territory to subject to the direct power of law. The legal response that follows such conceptual position is to create new laws to regulate new social phenomena by assuming the scheme – the law-maker creates the law and the regulatee yields to its power under the threat of punishment. Per se, such approach is natural, logical and relatively effective, at least it always has been in relation to our offline lives. After all, what else if not law passed and enforced by governments should order our behavior in social interaction be it offline or online. However, the assumption that social actors will obey law in cyberspace to the same degree as they have done offline for centuries is fundamentally flawed. This assumption is based on the expectation that law, if breached, can be enforced and the desirable social behavior can thus be achieved. Relatively true for the offline world, the enforcement is largely an unmanageable mission online. The nature of global online interaction is such, and legal scholarship is long aware of

2014, vol. 30, no. 1, pp. 142–147; see also RAND Corporation. *Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar* (rep.), 2014; Symantec Corporation. *Norton Cybercrime Insights Report: Understanding Cybercrime and the Consequences of Constant Connectivity* (rep.), 2016.

7 See RAND Corporation. *Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar* (rep.), 2014.

8 *Ibid*.

9 UK House of Commons, Home Affairs. *E-Crime* (rep.), 2013–2014. para. 24.

10 Despite the fact, that such approaches have long been suggest by numerous commentators, such as Lessig, Murray, Etzioni, Reidenberg, Reed, and others.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

it, that enforcement in the digital environment is problematic, to put it mildly. It is one thing to create legal infrastructure regulating online interaction (a task difficult enough) and quite another – to actually carry out the policy prescriptions, court orders, etc. With enforcement weak online, the human behavior seems to cast prudence to the winds.

As a hyper-connected global ecosystem, the internet is characterized by the decentralized power distribution where each participant is equally placed, oftentimes anonymously, in relation to the rest of the global network. All one needs to reach out to the global community or to create effects online and offline anywhere in the world is the access to the internet as well as obtainable technology. The achievement of similar results in the hierarchically structured, geo- and jurisdiction-determined physical reality would require immense resources. Online activity is notoriously difficult to prosecute not only because of the discrepancy between the global nature of online communication and the fragmented jurisdictional architecture on the planet but also because law enforcement is relatively unfamiliar with the technology.[11] It is only in the last few years that the law enforcement agencies of some jurisdictions have started recruiting IT specialists and establishing special offices entirely tasked with cybercrime control. Despite these efforts, the traditional justice systems were simply not designed to cope with the nature and the sheer scale of the wrongdoing online.

The question is – if we experience major difficulties with compliance online and enforcement is not a viable option to secure it, how can we address cybercrime and what should be the role of law in this enterprise? To answer this question, we need to closely look at the online deviance, the multifaceted phenomenon we are trying to address. Having gained insight into its nature, we can be better placed to offer regulatory solutions effective in addressing the reasons underlying the 'popularity' of online mischief. Such solutions may include a mixture of direct legal regulation (also known as command-and-control regulation), as well as indirect technological and socio-economic regulatory techniques shaped and coordinated by law.

This article examines the nature of online human interaction and explores regulatory powers, other than the law, that can influence human behavior online, such as the social norms, the design of technology, and the market. Building on

11 GALICKI, Alexander, HAVENS, Drew, PELKER, Alden. Computer Crimes. *American Criminal Law Review*, 2014, vol. p. 913.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

ideas of Lessig,[12] Murray,[13] Etzioni,[14] Reidenberg,[15] Reed[16] and others, the article offers an interdisciplinary attempt to formulate a framework of the holistic regulatory approach to cybercrime where all regulatory powers are engaged in a single comprehensive policy. In essence, the article offers a general framework and a vision of how cybercrime can best be addressed by any jurisdiction irrespective of its legal system.

We start with the brief overview of the challenges that the internet communication presents for the legal regulation in general.

2 Regulatory Idiosyncrasies of the Online Environment

2.1 Effectiveness of Enforcement Online

The usual regulatory reaction to the growing incidence of cybercrime was to create more laws in line with the traditional command-and-control approach assuming that such regulation would yield results similar to those that this approach yields offline.

Based on command-and-control philosophy, traditional regulation is dependent on effective inspection of the regulatory environment, detection of the non-compliance and subsequent enforcement by application of relevant polices, rules and tools in order to deter undesirable behavior.[17] Traditional legal model has been having difficulties adapting to the new realities marked by the speedy arrival of information society.[18] There is a number of reasons to question the effectiveness of overreliance on traditional approaches. We can try to achieve control by motivating citizens not to engage in certain behavior through imposition of restrictions, breaking which implies suffering consequences in terms of apprehension and punishments.[19] For that, the regulatory system needs to ensure the detection and enforcement are done at least to the level that the prospects of such enforcement influence the behavior of individuals. In economic terms,

12 LESSIG, Lawrence. *Code Version 2.0*. New York: Basic Books, 2006.

13 MURRAY, Andrew. *The Regulation of Cyberspace: Control in the Online Environment.* Abingdon: Routledge-Cavendish, 2007; MURRAY, Andrew, SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. *The Modern Law Review*, 2002, vol. 65, no. 4.

14 ETZIONI, A. Social Norms: Internalization, Persuasion, and History. *Law and Society Review*, 2000, vol. 34.

15 REIDENBERG, Joel. Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*, 1996, vol. 45; REIDENBERG, Joel. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, 1998, vol. 76.

16 REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.

17 ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 16; BALDWIN, Robert, CAVE, Martin, LODGE, Martin. *Understanding Regulation: Theory, Strategy, and Practice.* Oxford: Oxford University Press, 2012, p. 227.

18 MURRAY, Andrew. *Information Technology Law*. Oxford: Oxford University Press, 2013, p. 37.

19 GHOSH, Smith, TURRINI, Elliot. *Cybercrimes: A Multidisplinary Analysis*. Hedelberg: Springer, 2010, p. 366,

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

the risk of detection and conviction needs to be high enough and the incidence of enforcement frequent enough to make lawful behavior more rational than breaking the law. In other words, there should be a great likelihood that a single infringement of the law online can be investigated and enforced.[20] Considering, for example, that 11.6% of the world population are allegedly involved in copyright infringement it is virtually impossible to commence legal proceedings against such numbers.[21] The physical capacity and ability of the law enforcement to secure detection and conviction are simply not high enough.

This does not mean, however, that enforcement is a useless regulatory factor altogether. It only means that command-and-control approach cannot be the only instrument in our attempts to regulate behavior online. While of course the scare tactics may have some effect in informing the potential violators as to the consequences of their behavior, symbolic enforcement needs to be sustainable if effects are to last.[22] Luckily, technological developments indicate that better detection and enforcement is possible.[23]. These attempts however are doomed to stay symbolic given the sheer scale of online communication and online deviation that seem unmanageable for the institutions of the traditional justice system. Prosecutions in the cyberspace are prohibitively costly and ineffective for many jurisdictions. The challenges in identification and prosecution of cybercrime advocate against overreliance on fear of enforcement to deter attacks.[24] Hence, it would be wise to supplement this style by resorting to the utility of other regulatory powers that may facilitate higher levels of compliance. The law may need to redistribute its focus from almost delusional confidence that control and enforcement are realistically achievable online to the development of ethical behavioral standards online.[25]

20 REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012. pp. 54–55.

21 See *ibid*. at 55–58.

22 REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012, pp. 49–67.

23 The Danish Police's National Cybercrime Centre has implemented new technological methods that allow the Danish law enforcement to lift anonymity in the darknet and trace the bitcoin transactions. The new practice has already paid out in terms of securing convictions for drug dealers that use darknet to conduct their business. [Thastum, M. (2017, February 24). Gennembrud: Nye beviser ophaever kriminelles anonymitet pa morkenettet. Retrieved March 20, 2017, from http://www.anklagemyndigheden.dk/nyheder/Sider/gennembrud-nye-beviser-ophaever-kriminelles-anonymitet-paa-moerkenettet.aspx]

24 WELLINGTON, Katherine Booth. Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions. *Santa Clara High Technology Law Journal,* 2014, vol. 30, no. 1, p. 186.

25 REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

Even in the realm of ordinary deviation and crime, the regulation based on the traditional deterrence has limited effectiveness.[26] Robinson and Darley[27], for example, have argued that, "potential offenders do not know the law, do not perceive an expected cost for a violation that outweighs the expected gain, and do not make rational self-interested choices," and that, "the perceived probability of punishment is low, to the point where the threatened punishment is commonly not thought to be relevant to the potential offender."[28] The upshot of these observations is that the law regulates human behavior based on its normative appeal – that is when the message of the law is in accordance with the social consensus of the community about how its members should behave. In this sense, the effective law, the law that 'works' for the vast majority of its subjects is the law that mirrors social norms in place at a community in question. Citizens order their lives not in accordance with the laws but in accordance with what they believe the law is.[29]

In other words, the behavior consistent with the law is generated not so much by the law itself but by social and other extra-legal pressures of the community to which a potential offender belongs, as well as by internalized moral pressures.[30] Not that the law plays no role whatsoever, it does, of course. It is that the direct application of law is quite simply not the most effective form of regulation. If traditional command-and-control approach to regulation has had such difficulties in the physical reality, it produces even less effective outcomes in cyberspace.

2.2 Jurisdiction and Non-Territoriality

Ideally, the legal response to a global phenomenon should also be global. The apparent contradiction between the jurisdictional limitations of national laws and the actual global nature of the internet introduces yet another difficulty to effective regulation in the online environment.[31] States can subject foreign online actors to local laws, but the real prospects to secure compliance are insignificant without the cooperation of a foreign state involved, if it is willing and able to cooperate.[32]

---

26 GHOSH, Smith, TURRINI, Elliot. *Cybercrimes: A Multidisplinary Analysis*. Hedelberg: Springer, 2010, p. 366.

27 ROBINSON, Paul. The Role of Deterrence in the Formulation of Criminal Law Rules: At its Worst When Doing its Best. *Georgetown Law Journal*, 2003, vol. 91.

28 *Ibid*.

29 See *ibid*; also see REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.

30 BRAITHWAITE, John. Inequality and Republican Criminology. In HAGAN, John, PETERSON, Ruth. (eds.), *Crime and Inequality*. Stanfrod: Stanford University Press, 1995, pp. 283–284; also see ROBINSON, Paul, DARLEY, John. The Utility of Desert. *Northwestern University Law Review*, 1997, vol. 91.

31 ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 45.

32 *Ibid*. at 84; TRUDEL, Pierre. Jurisdiction over the Internet: A Canadian Perspective. *The International Lawyer*, 1998, vol. 32, p. 1047.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

The problem of national regulation and transnational activity is by no means new. Transnational trade, environmental pollution and migration all had to be accommodated within the limits of national laws.[33] Yet, the transnational online activity introduces a new aspect to the age-old issue. The effect that the jurisdictional divide produces on cybercrime is that of 'forum-shopping,'[34] when an offender engages in activity that may be legal in the hosting jurisdiction but illegal in the jurisdiction or multiple jurisdictions where the effects of online activity are most pronounced. At present, this is very much an insurmountable difficulty creating a chasmic distance between the enforcement efforts and their efficiency. In the absence of such legal infrastructure, however, some states attempt to regulate online activity on the basis of the effect doctrine rejecting the alternative doctrine that only that state from the territory of which particular online content originates has the right to exert its jurisdiction.

Perhaps one of the most famous early examples of the effect doctrine application is the French case of *LICRA & UEJF v. Yahoo! Inc & Yahoo France* (2000), where the French court ordered the US corporation and its French subsidiary to disallow online users from France to purchase Nazi memorabilia on yahoo.com auction from third parties. The court's ruling was based on the application of the French Criminal Code that prohibits any distribution of Nazi memorabilia. Despite the fact that yahoo.com, unlike yahoo.fr, is connected to the US audience much more than it is to the French, operating on the US servers and displaying content in English, the court held that the harm was suffered on the territory of France and because yahoo.com was accessible in France, French law was applicable to it as much as it was applicable to yahoo.fr.[35] Yahoo eventually complied with the requirement by removing the content from its yahoo.com website despite the fact that Nazi memorabilia are legal in the US. Following the logic of the French court, Yahoo or any other online actor is under obligation to remove any content or desist from any activity offending the laws of any other jurisdiction on the planet.

Arguably, the accommodation by yahoo.com of the decision of the French courts was based on voluntary compliance in pursuit of reputational considerations concerning its business in France rather than on any prospects of enforcement by the Paris court of its decision in the US.

In this regard, the behavior of businesses are much more visible online than that of individuals. Oftentimes operating anonymously online, individuals do not generally experience reputational pressures.

33 ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 24.

34 *Ibid*. at 23.

35 *LICRA v. Yahoo! Inc & Yahoo France* (Tribunal de Grands Instance de Paris, 22 May 2000); *LICRA & UEJF v. Yahoo! Inc & Yahoo France* (Tribunal de Grands Instance de Paris, 20 November 2000).

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

Coupled with the lack of enforcement, the problem is exacerbated by the "profound unwillingness of states to cooperate in development and enforcement of each other's criminal, revenue and other public laws"[36] in order to harmonize substantive and procedural legislation.[37] The alleged creator of the "I Love You" virus escaped prosecution in Philippines, his native country, because there were no laws penalizing the creation and/or distribution of computer viruses.[38]

One can speculate, however, that even if we have bridged the unbridgeable and overcome the gargantuan obstacle of jurisdictional divergence and managed to harmonize public laws on the global level, we would still have a problem. The practical difficulty will most certainly arise from the 'digital inequality' among the jurisdictions to speak the modern technological language – their capacities to investigate, probe into, collect and assess digital evidence quickly enough for it not to dissipate.[39] One thing is to have an access to the internet and another is to effectively use this access.

3 Who Are Cybercriminals?

Depending on the skill of the deviator, cybercriminals range from lone hackers who utilize basic techniques in pursuit of thrills and social group recognition, to malware developers, hactivists and organized groups, large organizations, and cyber terrorists that may engage highly sophisticated techniques in pursuit of a broad spectrum of interests and motives.[40] Rationales behind engaging in cybercrime are vast, ranging from pure intellectual curiosity and revenge to financial interests and political motives.[41]

Although the global population at large is reprehensive of the idea of cybercrime and its sheer progression, the moral attitude regarding online activity of many individuals who do not consider themselves criminals in everyday life shows somewhat disoriented moral attitudes. The Norton USA Human Impact report reveals that ordinary individuals who see themselves as law abiding citizens often regard such activities as illegal downloads, unauthorized access to personal information (email and browsing history), and unauthorized information shar-

36 ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 45.

37 *Ibid*.

38 GHOSH, Smith, TURRINI, Elliot. *Cybercrimes: A Multidisplinary Analysis*. Hedelberg: Springer, 2010, p. 230.

39 MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 95.

40 GHOSH, Smith, TURRINI, Elliot. *Cybercrimes: A Multidisplinary Analysis*. Hedelberg: Springer, 2010, p. 221; ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 272.

41 ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 277; see also ROGERS, Marcus, SEIGFRIED, Kathryn, TIDKE, Kirti. Self-Reported Computer Criminal Behaviour: A Psychological Analysis. *Proceedings of the Digital Forensics Workshop*. Elsevier, 2006.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

ing (sharing photographic images of other people) as acceptable.[42] Those who are engaged in this conduct do not perceive the commission of these and other similar acts online as deviation. Some forms of cybercrime are not perceived as something morally and ethically impermissible, unlike the classical 'physical' crime. Such conduct may be prohibited and penalized by law but the subject perceives this conduct as nothing deserving reprehension. Take for example the illegal downloading of MP3 audio files. If in ordinary social interaction we engage with moral and ethical standards through self-censoring anchored in understanding of the acceptable and the unacceptable, the online environment does not seem to provide a clear orientation in this regard. If stealing a CD from a music store is perceived by the society as unacceptable, such moral consensus does not seem to exist in regards the illegal digital music downloads. Many of those rare cybercriminals that are caught re-orient their attitudes and become law-abiding citizens helping law enforcement and assisting in improving security solutions.[43]

Not all episodes of cybercrime are the result of solely moral disorientation of law-abiding citizens in the online environment. A large share of online deviance is as deliberate as deviance offline. The inhibition of self-censoring system and moral disengagement in offline criminals are the result of a number of factors, such as social standing and class differences, psychological and psychopathological deficiencies, education, etc.[44] All these factors equally stand true for online deviance. However, online environment itself seems to contribute to cybercrime not only by the virtue of its technical idiosyncrasies but also by their psychological effects – the removal of our self-censoring mechanisms present in our daily social interactions.

4 Networks and Human Behavior

Before we can talk about the legal regulation of online behavior as such, we need to obtain a clear idea of how online environment influences human interaction. Is human behavior online in any way different from the behavior that we see in everyday physical social environment? If yes, then why?

When considering how humans act in the online environment, it is useful to keep in mind that online environment or cyberspace is not strictly speaking a space that one can physically enter. Rather, cyberspace or the internet is nothing else but a vast collection of data files stored on physical hardware infrastructure all over the globe. These data are continuously being retrieved, sorted, assembled together and interconnected by software algorithms. The process creates the coherent visual artefacts that we see on our computer and mobile screens,

42 Symantec Corporation (2016). *Norton Cybercrime Insights Report: Understanding Cybercrime and the Consequences of Constant Connectivity* (Rep.); Symantec Corporation (2010). *Norton Cybercrime Report: Human Impact* (Rep.).

43 ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 276.

44 GHOSH, Smith, TURRINI, Elliot. *Cybercrimes: A Multidisplinary Analysis*. Hedelberg: Springer, 2010, pp. 222, 226–227.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

and that we conceptualize as space.[45] The illusion of coherence applies to the web as a whole; the collected files and databases brought together create the internet appear as seamless environment that we navigate through.[46]

What we witness in fact is nothing else but the omnidirectional communication that happens almost instantaneously on the global scale. In this regard the term cyberspace or online environment does as much sense as telephone space or telephone environment. When we want to discuss human behavior online, we talk about communication that the internet provides and the effects that the morphology of this communication and the reduced nature of such communication have on human interaction.

The key element of the internet communication is its decentralized architecture with all participants "in constant dialog with each other."[47] Network, as the primary relationship model of the online environment determines its social structure. It replaces the hierarchical social morphology with horizontal. In contrast to the 'physical world', such architecture creates asymmetry in the geometry of power distribution, that is to say that any participant of communication gains access to communicating much greater results to much broader audience by means of the internet than he or she would have achieved offline.[48] Take as an example a hierarchical social structure of a classical corporation with a CEO as giving orders to subordinate managers which in turn instruct supervisors who give orders to workers. In contrast, a flow of power in a horizontal architecture of a network is distributed more evenly between the participants. Network communication is dynamic and open-ended because any participant has multiple connections to other participants.[49] Deleuze and Guattari determined the features of the network communication along the following lines:[50]

1. a network connects any point in its architecture to any other point.
2. a network is decentralized and nonhierarchical system without an organizing memory or central automation in that the network has no centre that is more important than any other part of the system.

45 See FATHERSTONE, Mike. Archiving Cultures. *British Journal of Sociology*, 2000, vol. 51, no. 1; MANOVICH, Lev. *The Language of New Media*. Cambridge, MA: MIT Press, 2001; PAUL, Christiane. The Database as System and Cultural Form: Anatomies of Cultural Narratives. In VESNA, Vicoria. (ed.), *Database Aesthetics*. Minneapolis: University of Minnesota Press, 2007; SNYDER, Ilana. New Media and Cultural Form: Narrative versus Database. In ADAMS, Anthony. and BRINDLEY, Sue. (eds.), *Teaching Secondary English with ICT*. London: Open University Press, 2007.

46 MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 21.

47 See MANOVICH, Lev. *The Language of New Media*. Cambridge, MA: MIT Press, 2001; MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 15.

48 MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 21.

49 Ibid. at 60.

50 DELEUZE, Gilles, GUATTARI, Felix. *A Thousand Plateaus: Capitalism and Schizophrenia*. London: Athlon, 1988, introduction; See also MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 26.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

3. it is reducible to neither the one nor the multiple in that it is neither a collection of individual things, not one large thing. Rather, a network, the internet in particular, is a multiplication of the infrastructure components, data and connections.[51]

The upshot is that nothing in this architecture can be fundamentally altered without altering the whole. One can remove thousands of websites, computers and servers from the web without having any effect on the architecture or the underlying algorithm of the whole.[52] Besides such structure is technically a daunting challenge for the traditional command-and-control regulation, it also has some peculiar psychological effects on its participants. Although human society has known of networked relationships such as friendship or trading networks, the online networking logic emphasizes reduced impersonal ties and connections rather than proximity of classical networks.[53]

In relation to the human community, Turkle puts it thus: "Networked, we are together but so lessened are our expectations of each other that we can feel utterly alone. There is a risk that we come to see each other as objects to be assessed – and only for the parts we find useful, comforting or amusing."[54] She argues that the emphasis on virtual interaction and the social pressure to be its part increase emotional distance. The reductive form of such interactions subsequently leads to our numbness to sensitivities, vulnerabilities, awkwardness and inefficiencies of others. Similarly, Silverstone and Orgad argue that while connectedness may increase closeness, it does not make it increase morality or responsibility in much the same way as physical proximity. Both argue that virtual digital communities have no basis in responsibility towards others but rather rely on mutual instrumental reciprocity.[55]

Miller takes this discussion even further and suggests that the arrival of the networked technology intensifies the pre-existing shortcomings of our social orientation rooted in our philosophy of the relationship between ourselves and the rest of the world.[56] He writes:

> Online life exaggerates the metaphysical conceptualization of presence upon which modern conceptions of being-in-the-world are based. This ultimately presents the world to us in instrumental terms, which,

51 BUCHANAN, Ian. Deleuze and the Internet. *Australian Humanities* Review, 2007, vol. 43.
52 See MURRAY, Andrew. *Information Technology Law*. Oxford: Oxford University Press, 2013, pp. 65–70.
53 MILLER, Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 60; CASTELS, Manuel. The Rise of the Network Society. Oxford: Blackwell, 2000, p. 19.
54 TURKLE, Sherry. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books, 2011, p. 154.
55 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 48.
56 *Ibid*. at 52.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

> in terms of ethics, means that beings in the world are approached primarily as things to be used.[57]

In this sense, human morals are essentially social product – the product that is generated by the interaction with others in physical context. The physical aspect of interaction removed, an individual may lose the sense of what is good and what is not in any new social setting. The distinction between good and bad is per se relative knowledge the generation of which requires physical interaction. Contemporary social media software emphasizes abstraction and digital 'dehumanization' through systemic and algorithmic approaches to online experiences in terms of reducing people to preformatted templates and categories, where the aesthetic and empathetic expression of humanness is largely lost.[58] The increasing mediation of social interactions through online environment challenges our tendencies to ground moral and ethical behavior in material context of mutual presence with fellow humans. Our sense of self as caring, moral and ethical beings is based on the material dimensions such as "being located in the body in proximity to other bodies and interacting with and caring for others in physical proximity to ourselves."[59] Such uninhibited behavior is attributable to whether or not such behavior forms a part of the group norms.[60] The online environment may strip a human being of the stimulus to be as empathetic as he or she is in the physical interactions. At the same time, the internet does not provide for the social norms that would motivate responsible and moral behavior, norms similar to those according to which we tend to order our offline behavior.

Professor Cass Sunstein in his book Republic.com suggested that the very nature of the internet isolates individuals behind screens rather than provides for community building.[61] In a space bounded by physical borders and physical activities people can navigate in a fixed symbolic order choosing their action in accordance with their knowledge of what is acceptable and what is not. With the arrival of the internet, this basic certainty of life easily accessible for interpretation has been blurred. Internet residents no longer are certain as to the permissibility of certain action, not only from the legal perspective but also from the perspective of morals and ethics.[62] The sense of imitation or simulation that internet inflicts makes both legal and moral orientation even more problematic.

---

57 *Ibid*.

58 GALLOWAY, Alexander. *The Interface Effect.* Cambridge, UK: Polity Press, 2012, p. 97; MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 106–108.

59 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 8

60 *Ibid*. at 38.

61 See SUNSTAIN, Cass. Republic.com. Princeton, NJ: Princeton University Press, 2002.

62 MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 35; MURRAY, Andrew. *Information Technology Law*. Oxford: Oxford University Press, 2013, p. 66.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

The environment in which the communication takes place affects any social communication, including online communication.[63] The communication is elaborated and completed by the symbolism of the surroundings, so that the same communication that takes place in a restaurant or on an airplane or online will have a very different 'charge' to it.[64]

4.1 Anonymity and Behavior

Another factor that contributes to uninhibited behavior is anonymity. Seen as central to the freedom of speech online, anonymity is also one of the biggest concerns.[65] Not only is anonymity (enhanced by encryption and cryptographic technologies) a problem from purely instrumental perspective of making a wrongdoer invisible or untraceable for the law enforcement, but also for its psychological effects on social behavior (removing the social stigma of lawbreaking). The prevailing psychological conception is that anonymity, coupled with the effects of online communication on human behavior that we have just covered, is primarily responsible for online abuse inevitably leading to unethical behavior.[66]

Anonymity of course is not all vice. Despite anonymity might seem a major inconvenience to regulatory efforts in the online environment, it is nonetheless vital for securing the right to privacy online. Any solution that involves curtailing anonymity must make sure the right to privacy is adequately protected.

There are many circumstances in which anonymity may be indispensable for the protection of a critically expressing individual, as for example in corporate criticism cases where an employee can be accused of 'defamation.' The sword of anonymity cuts both ways. The calls to legislative action, such as to unveil anonymity and to introduce more formal and thorough regulation of online communication, as well as of the internet as such, only will lead to targeting symptoms of the problem instead of addressing the core challenges.[67] It may hamper the advantages that the internet offers in terms of freedom of expression, and the access to information.

---

63 See LATOUR, Bruno. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press: Oxford, 2007.

64 *Ibid*.

65 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 5.

66 BISHOP, Jonathan. The Effect of De-Individuation of the Internet Troller on Criminal Procedure Implementation: An Interview with a Hater. *International Journal of Cyber Criminology*, 2013, vol. 7. no. 1, p. 28.

67 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, pp. 52–53.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

Different solutions are proposed – from the change in the nature of technologically mediated interaction to cultivation of moral and ethical standards in such interaction thorough education, to the use of market forces.[68]

5 Regulation of Online Behavior through Extra-Legal Influences

When the conventions of civil society are less apparent in the internet and where the law's authority cannot be imposed through enforcement, the law can still be accepted if actors choose to do so.[69] A norm created by a legislative act in such environment may not be recognized by online actors as introducing a meaningful instruction and may not be obeyed if this norm contradicts existing custom of non-compliance and the climate of permissiveness and impunity.[70] Grathoff claims that individuals generally see social convention, rather than the law, as imposing an obligation on them to behave in certain ways. The law according to him is only an organizing, crystalizing and sustaining agent the enforcement powers of which help social convention be visible, predictable and stable. "[I]t is the [social] convention that solves the moral coordination problem and so transmits the normative authority of morality to the social structure in question."[71] The internalized understanding that cybercrime breaches moral standards may trigger a silent psychological reaction resulting in behavioral reconsideration of one's actions.[72]

In practical terms this means thinking about construction of media morals and ethics that could address, as Miller puts it, the syndrome of "compassion fatigue," which would involve shared vulnerability and the willingness "to be troubled by our mediated experiences of others."[73] Arguably, this will generate a sense of community and responsibility. The law as an organizing agent can mandate standards in internet architecture, technology manufacturing, service providing, taxation, and most importantly in educational curricula in order to facilitate the development of the appropriate morals online.[74] While we are busy

68 LANIER, Jaron. *You are Not a Gadget.* New York: Vintage Books, 2010; BOOTHROYD, Dave. Touch, Time and Technics: Levinas and the Ethics of Haptic Communications. *Theory, Culture and Society*, 2009, vol. 26, pp. 330–345.

69 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 5; REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012, p. 105.

70 REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012, pp. 20, 129.

71 GARTHOFF, Jon. Legitimacy is not Authority. *Law and Philosophy*, 2010, vol. 29, no. 6, pp. 669–680.

72 GHOSH, Smith, TURRINI, Elliot. *Cybercrimes: A Multidisplinary Analysis*. Hedelberg: Springer, 2010, p. 374.

73 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 106.

74 See LESSIG, Lawrence. *Code Version 2.0*. New York: Basic Books, 2006; REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

looking for technical solutions to increase our control of the internet, we should not overlook to foster the network ethics that has a great potential to determine the 'rules of the game' online.[75] Law can play a central role in coordinating the appropriate regulatory efforts.[76]

Combination of legal and extra-legal regulatory techniques to achieve more effective outcomes is already used in such areas as environment that has long sought to gain compliance with the law not merely by resort to formal enforcement and prosecution but by using a mixture of techniques, such as education, advice, and persuasion.[77] Compliance approaches to enforcement as known in environmental law "emphasize the use of measures falling short of prosecution in order to seek compliance with laws."[78] The law can order or stimulate the effort to educate the potential offenders in a patient and open-minded way into complying with the social and legal norms.[79]

Lessig in his Code discusses social norms, market, and internet architecture as alternative regulatory modalities through which the human behavior can be influenced.[80] To illustrate his thesis, he refers to the regulation of smoking, where law can impose a ban on smoking, use taxation to influence the market of cigarettes, and include information on harm that results from smoking in education programs. As a technical solution, the law can also impose limitations on the amount of chemicals in cigarettes.[81] Murray suggests that by using Lessig's modalities in whatever degrees necessary, the desirable regulatory results can be achieved with regard to the behavior online.[82]

Murray and Scott have developed Lessg's ideas and proposed the following categorization of regulatory forces. They refer to these categories as "control systems"[83]:

- hierarchical control (law);
- community-based control (social norms):

75 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 107.

76 See REIDENBERG, Joel. Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*, 1996, vol. 45; REIDENBERG, Joel. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, 1998, vol. 76.

77 BALDWIN, Robert, CAVE, Martin, LODGE, Martin. *Understanding Regulation: Theory, Strategy, and Practice.* Oxford: Oxford University Press, 2012, p. 238.

78 *Ibid*. at 239; also see RICHARDSON, Genevra. *Policing Pollution: A Study of Regulation and Enforcement.* Clarendon Press: Oxford, 1983.

79 BALDWIN, Robert, CAVE, Martin, LODGE, Martin. *Understanding Regulation: Theory, Strategy, and Practice.* Oxford: Oxford University Press, 2012, p. 239.

80 See LESSIG, Lawrence. *Code Version 2.0*. New York: Basic Books, 2006.

81 *Ibid*.

82 MURRAY, Andrew. *Information Technology Law*. Oxford: Oxford University Press, 2013, p. 61.

83 MURRAY, Andrew, SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. *The Modern Law Review*, 2002, vol. 65, no. 4, p. 491.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

- competition-based control (market);
- design-based control (architecture).

5.1 Social Norms And Morals Of The Community-Based Control System

Back in 1997, Tracey Meares wrote: "it is time for us to take seriously the notion that social norms are better and more effective constraints on behavior than law could ever be. It is time to give norms a chance."[84] Social norms not only constrain behavior externally by subjecting the actor to the community's expectations but also influence the actor's identity, worldview and the self-image. All this in turn influences the direction in which the actor makes individual choices if left to his or her own devices.[85]

Etzioni provides an example of a Jewish butcher living in an orthodox Jewish community who is unwise enough to decide to sell pork. From the perspective of external social control, the butcher would soon learn that the violation of strongly held social norms lead to the loss of business and social marginalization. From the perspective of internal predispositions shaped by these same social norms, the butcher would perhaps dismiss the idea of selling pork without any serious consideration the moment it crossed his mind, for it would be in gross violations of his values and his self-image.[86] Morals undoubtedly play an important role as intrinsic factor of our self-censorship.

Some commentators suggest that we need to concentrate on transforming the internet's 'global village' into a moral community.[87] For that to happen, we need to expand the 'natural habitat' of social norms as it exists in our immediate physical interactions to our communication online. This is especially important in regards those whom we do not know, because, sadly, our social empathy, pity or care that we tend to exhibit towards our immediate physical contacts have not expanded to the same degree for the 'mediated' others with whom we engage online.[88]

To demonstrate, Miller provides some evidence. In 2010, a 42-year-old Simone Back posted a status on her Facebook: "took all my pills, be dead soon, bye-bye everyone." This post provoked a discussion on her Facebook wall, where some of her 1082 connections debated over the sincerity of this suicide attempts while some warned the participants that if the attempt was in fact genuine they

84 MEARES, Traey. Drugs: It's a Question of Connections. *Valparaiso Review*, 1997, vol. 31, p. 594.

85 ETZIONI, A. Social Norms: Internalization, Persuasion, and History. *Law and Society Review*, 2000, vol. 34, no. 1, p. 161.

86 *Ibid*. at 163.

87 SMITH, David. *Moral Geographies: Ethics in a World of Difference*. Edinburgh: Edinburgh University Press, 2000.

88 BAUMAN, Zygmunt. *Postmodern Ethics.* Oxford: Blackwell, 1993; BOLTANSKI, Luc. *Distant Suffering: Morality, Media and Politics*. Cambridge University Press: Cambridge, UK, 1999.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

would soon regret the comments. Seventeen hours later, Simone's mother having learned of her last status update on Facebook contacted the police. Police found her dead shortly after. None of her friends on Facebook, even those who resided nearby, attempted to contact Simone by the phone or to visit her. The reason behind such manifestly bizarre behavior of Simone's 'friends' might not be the fact that they were bad people. Rather it may be pointing to the fundamental disorientation in care and responsibility. Those who took part in the discussion on Simone's wall were allegedly affected by the abstracted and objectified online environment where existing social norms can be effectively triggered.[89]

In 2008, a 19-year-old Abraham Biggs took his life while streaming his suicide live on justin.tv. Of some 1500 spectators who witnessed his death, some encouraged him to do so, some berated.[90] In 2013, a student at the University of Guelph, Canada, announced on *4chan* he would be committing suicide on live video stream. A *4chan* member set up a video chat room on another website to accommodate 200 witnesses. When the number was reached, the young man took his life. The comments both in the chat room and on *4chan* exhibited uncommon distance and coldness to the unfolding events with witnesses concerned more with the visibility of the events rather than with the fact that a human being is taking his life.[91] While it would be inaccurate to allege that these episodes exhibit the wicked human nature unrestrained by social conventions of the physical reality – for after all such online 'shows' may attract a very particular audience rather than a fairly spread and diverse members of society – the examples are shocking. Moreover, it appears that these disturbing incidents are growing in numbers versus stable incidence rate of the face-to-face contact incidents. It is a real trend rather than a number of random incidents.[92]

It is hard to ignore the fact that social norms are perhaps one of the most powerful regulatory instruments that has a real prospect of addressing the underlying problems of the abovementioned issues, first and foremost through education in its broadest sense. In the context of addressing the online mischief in general and dehumanizing attitudes among the online actors in particular, education may facilitate understanding of the link between online actions and their real world manifestations.

5.2 Market of the Competition-Based Control System

Market control is another powerful force that may address and shape online behavior. It aims to deploy economic or other market advantages in order to influence behavioral preferences. Economic pressures can raise the cost of online

89 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 32.

90 *Ibid*.

91 Ibid. at 32–33.

92 See LANIER, Jaron. *You are Not a Gadget.* New York: Vintage Books, 2010.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

mischief through reshaping the economic considerations of engaging in antisocial online activity. For example, the advance of the legal, affordable and convenient online MP3 sales and/or streaming on such platforms as Spotify or iTunes render the illegal download services uncompetitive and meaningless. The market regulation has addressed this problem of illegal services more efficiently than the command-and-control technique could ever hope.[93]

Even the early architectural solution to the problem of illegal file-sharing services could not achieve results as impressive. Back in the days of CDs, the music industry designed the Digital Rights Management software (DRM), such as Cactus Data Shield, Sony Extended Music Protection or Apple's FairPlay to protect the copyrights and derail the illegal file-sharing activity. Despite being reinforced by the legal provisions, these systems failed to equal the hopes of the music industry. The multiple technical difficulties and design flaws made these systems inoperable on a large market scale as they would prove incompatible with certain platforms or operating systems. At the end of the day, the DRM protection became valueless.[94]

Although these examples provide a good illustration of the market self-regulation and the potential of the market forces to generate balance with time, this approach has its downsides. If we have online behavior left entirely to the market influences, the unprofitable social values would most probably be left out of consideration.[95] The law can direct the market forces by creating a system of incentives and restraints through, for example, well-known taxation and licensing techniques.[96] The imposition of or exemption from taxes and application of licenses with regards to design and development of technology, or access to it, can prove equally effective in regards both the industry and individuals.

5.3 Architecture and Code Of The Design-Based Control System

Internet communication as well as the software technology is in nature a numerical representation of binary 0–1 digital code which is programmable, alterable and subject to algorithmic manipulation. In consequence, "it can be easily manipulated, customized, copied and transferred between different sources, objects and means of technological delivery"[97] Architectural solutions can play a significant role in hedging the undesirable online activity, stimulating the

93 MURRAY, Andrew. *Information Technology Law*. Oxford: Oxford University Press, 2013, pp. 62–65.

94 *Ibid*. at 62–65.

95 KESAN, Jay, SHAH, Rajiv. Deconstructing Code. *Yale Journal of Law and Technology*, 2004, vol. 6, p. 388.

96 KATYAL, Neal. Criminal Law in Cyberspace. *University of Pennsylvania Law Review,* 2001, vol. 149, p. 1041.

97 MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011, p. 15; also see MANOVICH, Lev. *The Language of New Media*. Cambridge, MA: MIT Press, 2001.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

market in certain directions and stimulating the migration of the social norms into the online environment.[98]

Unlike with other regulatory forces, manipulation of architectural standards offers, at least in theory, ex ante control over the behavior of online actors by erecting defenses and making online security structures hard and costly to circumvent.[99] This may seem a very attractive option. However, as we have seen in the DRM examples above, the direct regulation of the code may not necessarily yield any lasting results. Although the code regulation seems to be the perfect way to achieve compliance by ruling out unacceptable technological manipulations, the nature of the code itself stands on the way – the malleability of the code can be used for both erecting the defenses and taking them down.

Crude technical solutions may also fail to produce acceptable result due to its indiscriminate effects. Consider for example a classical DDoS attack, which in essence is a number of request packets being sent to a server. It is a daunting technological challenge to differentiate between an actual attack and an actual interest of a large number of individuals genuinely requesting information on a certain issue. The only differentiator here appears to be the intent of the sender,[100] verifying which in an event as massive as DDoS attack is an impossible task.

Some commentators voice concerns that while the code gives a convenient opportunity to restraint certain behavior, it raises issues of over-regulation.[101] Brownsword, for example, argues that the internet architecture's proposed immutability would clash with the values of a liberal society where freedoms extend to the freedom in choice whether an individual wishes to comply with the law at all.[102] The removal of a choice not to be bad takes from us the possibility of being good by refraining from committing delinquencies.[103] Besides being illiberal the code makes a too tough of a tool for regulation allowing for no flexibility or other interests to be taken into account, such as for example 'fair use' in copyright regulation.[104]

Architectural solutions however can contribute to influencing the will through other subtler means, such as the design of humanness-friendly internet by means of haptic technologies[105] that could address the dehumanization and objectification of online communication as discussed above. Architecture-ori-

98 REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.

99 *Ibid*. at 207.

100 MULLIGAN, Deirdre, SCHNEIDER, Fred. Doctryne for Cybersecurity. *Daedalus, the Journal of the American Academy of Arts and Sciences*, 2011, vol. 140, no. 4, p. 83.

101 See BROWNSWORD, Roger. Code, Control and Choice: Why East is East and West is West. *Legal Studies*, 2005, vol. 25.

102 Ibid. at 20.

103 Ibid.

104 ROWLAND, D. *Information Technology Law.* London: Routledge, 2017, p. 13.

105 See PETERSEN, Mark. *The Senses of Touch: Haptics, Affects and Technologies.* New York: Berg Publishers, 2007.

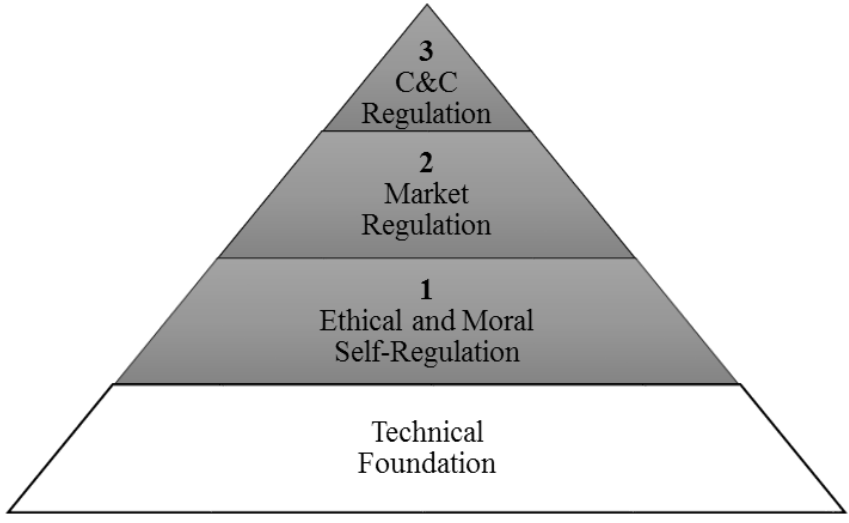
Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

ented solutions that target ethics and humanness of online experiences may not only address the deeper underlying source of the problem of antisocial behavior online, but also will not compromise freedom, communication and autonomy, which is what restrictive architectural solutions tend to do.[106]

While code might not be a perfect solution to addressing cybercrime, or it might not even be comparable to the law (as what Lessig suggests), it still offers a valid opportunity to contribute to drawing the line of the permissible, especially in circumstances where a mature moral attitude towards undesirable online behavior has not yet formed.

6 A Possible Holistic Regulatory Regime

How can the law respond to the challenges of ever-increasing cybercrime? How can it contribute to ordering the online social realities when the traditional approached based on classical command-and-control regulation is no longer a viable option? The answer to these questions is a public policy based on a holistic regulatory regime. To be effective in regulation of online behavior, such regime needs to comprise an array of regulatory techniques. The traditional command-and-control technique must be complemented with the forms of indirect regulation – the community, competition and design-based regulation. United by the framework of a single regime, each of the regulatory powers can address different levels of online human interaction. Schematically, it can be presented as a pyramid.



106 MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016, p. 113.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

The technical solutions can provide for the basic defense barrier outlining the absolute minimum-security standards for digital infrastructure. It is the foundational level and as such is not considered as regulating but rather as setting the technical boundaries of permissible. As mentioned, technological design can also be used to provide for haptic experience online, which will address objectification and dehumanization of online interaction.

The first level of the pyramid is our internalized moral and ethical predispositions regarding the wrong and the right in the online communication. This level is the community-based control that effects moral and ethical attitudes towards online activity through education and learning. The second level of influence picks up where the morals failed. The market control motivates online actors by appealing to them through economic means. Finally, the third level of command-and-control direct legal regulation is providing for both the coordination of the lower level control systems and punitive action against those who chose to deviate.

The role of the governmental authority in such a model is that of a coordinating visionary engaging all regulatory powers and streaming them into a single regulatory effort by using law. It is important to keep in mind that the community-based regulatory forces as outlined above will likely develop and change under the influence of the regulatees themselves. It is also likely that the law will experience pressures from these regulatory powers and change accordingly, just like all regulatory powers will influence and change each other. None of the regulatory modalities is likely to prove sufficient if disjoint and uncoordinated. Only together they can achieve a long lasting effective result. This is perhaps the most important consideration that the policy- and law-makers need to take on board in generating the regulatory strategy for cyberspace. In the words of Braithwaite: "[t]o reject punitive regulation is naïve, to be totally committed to it is to lead a charge of the light brigade. The trick of successful regulation is to establish a synergy between punishment and persuasion."[107]

Coordination, organizational reform and learning are the remedies for our current failures.[108] Some countries may already have various regulatory agencies in place that effect policies in all the areas we have discussed. However, existing state regulators often use inconsistent polices in regards overlapping jurisdictional regimes or omit certain areas because these areas fall out of their regulatory practice. Such complexities in regulation are often the cause of 'normalization of deviance.'[109] The coordinating function of a holistic regulatory policy can correct these shortcomings. Many countries have already adopted legal frameworks

107 AYRES, Ian, BRAITHWAITE, John. *Responsive Regulation*. Oxford: Oxford University Press, 1995, p. 25.

108 BALDWIN, Robert, CAVE, Martin, LODGE, Martin. *Understanding Regulation: Theory, Strategy, and Practice.* Oxford: Oxford University Press, 2012, pp. 78–80.

109 *Ibid*. at 78

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

in different areas of law pertaining to the information and network technologies, including criminal and civil laws, as well as criminal and civil procedures. The problem here is not so much in legislating but in coordinating. The challenge is to provide for sustainable channels of collaboration between agencies that execute this holistic regulatory policy.

7 Conclusion

Being the principal infrastructure of the modern times, it is inevitable that the internet will continue to be the main medium of human interaction, and the main source of our advances and problems alike. It is greatly important that we rightly assess the implications of the effects that online interaction has on our behavior and subsequently on our socio-economic environment. The attempts to address cybercrime – that so far have been primarily founded on a traditional approach to regulation – have failed. We have extended great efforts in trying to control the runaway incidence of cybercrime by piecemeal action. We create more laws and we produce technical security solutions. However, we apply little effort to unite and coordinate these attempts in dealing with cybercrime on the basis of understanding the underlying condition of this phenomenon. Social norms and morals are largely disregarded in relevant policy considerations in the vast majority of jurisdictions worldwide. We require a public policy that can mobilize all regulatory regimes in order to address cybercrime. By connecting the command-and-control power of law to other regulatory powers that operate within the society, we will be able to address cybercrime and to provide for an effective, sustainable and balanced ordering of online interaction.

The pure, ontologically separate understanding of law needs to give way to a more systemic and holistic approach where politics, morality, justice, technology, and cultural norms are forces of a single regulatory effort. In a way, the emergence of the internet forces us to reconsider the classical top-down approach to legal regulation due to its obvious inefficiencies online and return to the incorporation of the bottom-up community-produced legal custom. The law cannot simply prescribe it should develop or facilitate development of behavior online by addressing the formation of relevant underlying values. The focus should be on interaction of law and society rather than the law's control of the society.

References (alphabetical order)

AYRES, Ian, BRAITHWAITE, John. *Responsive Regulation*. Oxford: Oxford University Press, 1995.

BALDWIN, Robert, CAVE, Martin, LODGE, Martin. *Understanding Regulation: Theory, Strategy, and Practice.* Oxford: Oxford University Press, 2012.

BAUMAN, Zygmunt. *Postmodern Ethics.* Oxford: Blackwell, 1993.

BISHOP, Jonathan. The Effect of De-Individuation of the Internet Troller on Criminal Procedure Implementation: An Interview with a Hater. *International Journal of Cyber*

Criminology, 2013.
BOLTANSKI, Luc. *Distant Suffering: Morality, Media and Politics*. Cambridge University Press: Cambridge, UK, 1999.
BOOTHROYD, Dave. Touch, Time and Technics: Levinas and the Ethics of Haptic Communications. *Theory, Culture and Society*, 2009, vol. 26
BROWNSWORD, Roger. Code, Control and Choice: Why East is East and West is West. *Legal Studies*, 2005, vol. 25.
BUCHANAN, Ian. Deleuze and the Internet. *Australian Humanities* Review, 2007.
CASTELS, Manuel. The Rise of the Network Society. Oxford: Blackwell, 2000.
DELEUZE, Gilles, GUATTARI, Felix. *A Thousand Plateaus: Capitalism and Schizophrenia*. London: Athlon, 1988.
ETZIONI, A. Social Norms: Internalization, Persuasion, and History. *Law and Society Review*, 2000, vol. 34, no. 1.
FATHERSTONE, Mike. Archiving Cultures. *British Journal of Sociology*, 2000, vol. 51, no. 1.
GALICKI, Alexander, HAVENS, Drew, PELKER, Alden. Computer Crimes. *American Criminal Law Review*, 2014, vol. p. 913
GALLOWAY, Alexander. *The Interface Effect.* Cambridge, UK: Polity Press, 2012.
GARTHOFF, Jon. Legitimacy is not Authority. *Law and Philosophy*, 2010, vol. 29, no. 6.
GHOSH, Smith, TURRINI, Elliot. *Cybercrimes: A Multidisplinary Analysis*. Hedelberg: Springer, 2010.
HAGAN, John, PETERSON, Ruth. (eds.), *Crime and Inequality*. Stanfrod: Stanford University Press, 1995
KATYAL, Neal. Criminal Law in Cyberspace. *University of Pennsylvania Law Review,* 2001, vol. 149.
KESAN, Jay, SHAH, Rajiv. Deconstructing Code. *Yale Journal of Law and Technology*, 2004, vol. 6.
LANIER, Jaron. *You are Not a Gadget.* New York: Vintage Books, 2010.
LATOUR, Bruno. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press: Oxford, 2007.
LESSIG, Lawrence. *Code Version 2.0*. New York: Basic Books, 2006.
MANOVICH, Lev. *The Language of New Media*. Cambridge, MA: MIT Press, 2001.
MEARES, Traey. Drugs: It's a Question of Connections. *Valparaiso Review*, 1997, vol. 31.
MILLER Vincent. *Understanding Digital Culture*. London: SAGE Publications, 2011.
MILLER, Vincent. *The Crisis of Presence in Contemporary Culture: Ethics, Privacy and Speech in Mediated Social Life.* Los Angeles: SAGE Publications, 2016.
MULLIGAN, Deirdre, SCHNEIDER, Fred. Doctryne for Cybersecurity. *Daedalus, the Journal of the American Academy of Arts and Sciences*, 2011, vol. 140, no. 4.
MURRAY, Andrew, SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. *The Modern Law Review*, 2002, vol. 65, no. 4.
MURRAY, Andrew. *The Regulation of Cyberspace: Control in the Online Environment*. Abingdon: Routledge-Cavendish, 2007
MURRAY, Andrew. *Information Technology Law*. Oxford: Oxford University Press, 2013.
PAUL, Christiane. The Database as System and Cultural Form: Anatomies of Cultural Narratives. In VESNA, Vicoria. (ed.), *Database Aesthetics*. Minneapolis: University of Minnesota Press, 2007.
PETERSEN, Mark. *The Senses of Touch: Haptics, Affects and Technologies.* New York: Berg Publishers, 2007.

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601

REED, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.
REIDENBERG, Joel. Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*, 1996, vol. 45.
REIDENBERG, Joel. Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*, 1998, vol. 76.
RICHARDSON, Genevra. *Policing Pollution: A Study of Regulation and Enforcement.* Clarendon Press: Oxford, 1983.
ROBINSON, Paul, DARLEY, John. The Utility of Desert. *Northwestern University Law Review*, 1997, vol. 91
ROBINSON, Paul. The Role of Deterrence in the Formulation of Criminal Law Rules: At its Worst When Doing its Best. *Georgetown Law Journal*, 2003, vol. 91
ROGERS, Marcus, SEIGFRIED, Kathryn, TIDKE, Kirti. Self-Reported Computer Criminal Behaviour: A Psychological Analysis. *Proceedings of the Digital Forensics Workshop*. Elsevier, 2006
ROWLAND, D. *Information Technology Law.* London: Routledge, 2017.
SMITH, David. *Moral Geographies: Ethics in a World of Difference*. Edinburgh: Edinburgh University Press, 2000.
SNYDER, Ilana. New Media and Cultural Form: Narrative versus Database. In ADAMS, Anthony. and BRINDLEY, Sue. (eds.), *Teaching Secondary English with ICT*. London: Open University Press, 2007.
SUNSTAIN, Cass. Republic.com. Princeton, NJ: Princeton University Press, 2002.
TRUDEL, Pierre. Jurisdiction over the Internet: A Canadian Perspective. *The International Lawyer*, 1998, vol. 32
TURKLE, Sherry. *Alone Together: Why We Expect More from Technology and Less from Each Other*. New York: Basic Books, 2011
WELLINGTON, Katherine Booth. Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions. *Santa Clara High Technology Law Journal,* 2014, vol. 30, no. 1

Published by Palacký University Olomouc, Czech Republic, 2017.
ISSN (print): 1213-8770; ISSN (online): 2464-6601