# EXPOSING THE ICT REGULATORY DILEMMA: THE TEST FOR GOVERNMENTS

Mzukisi Njotini
*LLB LLM LLD*
*Associate Professor, Department of Private Law*
*University of Johannesburg*

**SUMMARY**

Information and Communications Technologies (ICTs) generate both benefits and challenges for society. For example, ICTs augment social development and encourage equality and inclusivity. In addition, these technologies create a new space – that is, cyberspace. This space is separate from physical or offline space. The emergence of this space has resulted in regulators having difficulty establishing suitable regulations. The latter are regulations that understand the workings and dynamics of ICTs. Mostly, regulators adopt regulatory frameworks that are suitable for controlling physical or offline environments. These regulations accept, *inter alia*, that the source of regulating is the law or legal rules. In the main, regulators continuously re-invent the ICT regulatory wheel in the hope that, by chance, suitable ICT regulations will emerge or be found. Consequently, ICT regulations often exacerbate the existing ICT regulatory dilemma. This article examines an alternative approach to regulations that is external to the law or legal rules. The structure accepts that a proper ICT regulatory framework is one that understands the workings and dynamics of these technologies. Given this understanding, ICT regulations should be bound to the technology and be able to develop or evolve with it.

## 1 INTRODUCTION

Information and communications technologies (ICTs) generate opportunities for society. Specifically, the Internet of things (IoT)[1] alone is likely to contribute 14 trillion US dollars to the global economy by 2030.[2] This contribution has the effect of intensifying economic development, lessening

[1] IoT is a combination of the Internet and things – for example, gadgets, smart devices, human beings, and hardware. See Minteer *Analytics of the Internet of Things* (2017) 14–15 and Khidadadi, Dastjerdi and Buyya "Internet of Things: An Overview" in Buyya and Dastjerdi (eds) *Internet of Things: Principles and Pradigms* (2016) 3 3. It measures, digitally controls and deals with the convergence of "previously unconnected things, reaching people and objects that technology could previously not reach and in the process also supports sustainable development element". See Vermesan and Friess *Internet of Things: From Research and Innovation to Market Development* (2014) 3 and World Economic Forum "Internet of Things: Guidelines for Sustainability" https://www.weforum.org/whitepapers/internet-of-things-guidelines-for-sustainability (accessed 2018-10-10).

[2] Häuser "Digital Business, Autonomous Systems and the Legal Challenges" 2014 2 *Internet & Law* 26 26–27.

inequality and encouraging inclusivity.[3] Because these technologies are comprehensive and inter-connected,[4] they have become instrumental in facilitating compliance with the United Nation's Sustainable Development Goals – for example, ending extreme poverty, improving quality of life and fostering innovation.[5] Despite these contributions, shortcomings in technology regulations, limited societal innovation and the uneven adoption of technologies undermine the opportunities that ICTs produce. As regards technology regulation, the cardinal view on the process of regulating is that the law or legal rules regulate.[6] In this manner, law prescribes the limit and extent to which society ought to conduct itself. It also "tells individuals not to deduct more than 50% of the cost of business meals from their income tax; it tells corporations not to resist unionisation; it tells police not to coerce confessions from suspects".[7] In this regulatory exercise, the State or government plays an indispensable function.[8] Specifically, the State relies on tools of detection and effecting for regulatory or governance purposes.[9]

Tools of detection largely enable government to gather information about those who are regulated – that is, society – and, using state channels, affect the behaviour of society towards a particular desired end.[10] For example, in cases where an allegation of wrongdoing is made, the State investigates (using tools of detection). The rationale is to guarantee that the elements of the alleged wrongdoing are present. Thereafter, it imposes (using tools of effecting) a sanction – that is, the threat of *ex post facto* punishment[11] – on those who defy or disobey the established legal rules. By so doing, the State follows the command-and-control procedure[12] wherein the law is a structure in terms of which legal rules are employed to control the activities of society and (legal) sanctions are imposed on those who transgress the law.[13]

---

3 Minteer *Analytics of the Internet of Things* 14–15 and Khidadadi, Dastjerdi and Buyya in Buyya and Dastjerdi *Internet of Things: Principles and Pradigms* 3 3.

4 Okin *The Internet Revolution: The Not-For-Dummies Guide to the History, Technology, and Use of the Internet* (2005) 19; and Reed *Internet Law: Text and Materials* 2ed (2004) 8.

5 See United Nations Development Programme (UNDP) "Sustainable Development Goals" http://www.undp.org/content/dam/undp/library/corporate/brochure/SDGs_Booklet_Web_En.pdf (accessed 2018-10-10).

6 Black *Critical Reflections on Regulation* (2002) 2; and Ding "Internet Regulation" in Campbell, C Bán, S Bán and Szabo (eds) *Legal Issues in the Global Information Society* (2005) 279 281–282.

7 Lessig "The Constitution of Code: Limitation on Choice-Based Critiques of Cyberspace Regulation" 1997 5 *CommLaw Conspectus* 181 181.

8 Torfing *Politics, Regulation and the Modern Welfare State* (1998) 142.

9 Hood and Margetts *The Tools of Government in the Digital Age* (2007) 2.

10 Hood and Margetts *The Tools of Government in the Digital Age* 3.

11 Lessig 1997 *CommLaw Conspectus* 181.

12 Baldwin and Cave *Understanding Regulation: Theory, Strategy, and Practice* (1999) 1–2; and Coglianese and Mendelson "Meta-Regulation and Self-Regulation" in Baldwin, Cave and Lodge (eds) *The Oxford Handbook of Regulation* (2010) 146 146.

13 Black *Critical Reflections on Regulation* 2. The basis of the command-and-control procedure is that "law … shows a man (or woman) the way to a righteous life on earth, a socially acceptable secular behaviour; for completion of man's (or woman's) destiny on the supernatural level". See Strömholm *A Short History of Legal Thinking in the West* (1985) 111. The above-mentioned is the case because "law is nothing else than a rational ordering of things which concern the common good, promulgated by whoever is in charge with the care of community". See Aquinas "Law and the Common Good" in Kent (ed) *Law and Philosophy: Readings in Legal Philosophy* (1970) 552.

Watson provides one of the finest descriptions of the above-mentioned structure by stating that legal rules

> "[c]laim[ ] to be authoritative, the rules are part of a system, the system claims jurisdiction in a wide range of matters, the rules elicit obedience, and the rules are or derive from a sovereign's command".[14]

One of the prominent features of the command-and-control system is that it is mostly stagnant and cumbersome.[15] It usually arises in situations where there is already a legal dispute. A legal process is then commenced to react to the established dispute.[16] Furthermore, the command-and-control system requires strict observance to certain accepted sets of rules. An examination of the law-making process in South Africa can be used as an example. This process is contained in Chapter 4 of the Constitution of the Republic of South Africa, 1996 (Constitution). The law-making process begins with a discussion document referred to as a Green Paper. The Green Paper is followed by a second document known as a White Paper, which generally formulates the policy programmes of the State. Thereafter, a Bill that includes a draft version of the envisaged law is prepared.[17] The Bill is tabled in the National Assembly, or the National Council of Provinces, for consideration by the members. Subsequently, it is referred to the related committee or committees of the National Assembly, or National Council of Provinces, and published for public comment in the *Government Gazette*. The latter committees debate the Bill and make certain modifications, if necessary. The last stage of the law-making process is to have the Bill assented to and signed into law by the President.[18]

Given the rigidity of the law-making process, the legal rules that inform it are likely to fail to deal sufficiently with conventional challenges. In this article, the most pertinent of these challenges relate to those that are generated by ICTs.[19] The examples include phishing, computer cracking,

---

14 Watson *The Nature of Law* (1977) 35.

15 Barlow "Selling Wine Without Bottles: The Economy of Mind on the Global Net" http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/idea_economy_article.html (accessed 2016-10-13).

16 Watson *The Nature of Law* 18.

17 Various types of Bill may be distinguished – namely: Ordinary Bills (s 75 Bills), Ordinary Bills that affect provinces (s 76 Bills), Money Bills (s 77 Bills) and Constitutional Amendments (s 74 Bills). See Parliamentary Monitoring Group (PMG) "The Legislative Process" http://www.pmg.org.za/parlinfo/sectionb3 (accessed 2016-11-2).

18 Ss 74(9), 75(1)(*d*) and 76(1)–(3) of the Constitution. It is important to note that the provision of assenting to and signing of Money Bills by the President is not expressly set out in the Constitution. See s 77 of the Constitution.

19 The term "ICTs" is usually described differently to the word "technology" – that is, the "material artifacts (objects, devices, processes etc.) as well as the knowledge concerning these artifacts, and the activity aiming at the satisfaction of particular human and social needs through devising appropriate artifacts as well as the knowledge concerning this activity". See Arageorgis and Baltas "Demarcating Technology From Science: Problems and Problem Solving in Technology" 1989 XX *Zeitschrift für Allgemeine Wissenschaftstheorie* 212. ICTs refer, *inter alia*, to the Internet and the World Wide Web or Web. On the one hand, the term "Internet" refers to the interconnected system of networks that connect computers around the world using the Transmission Control Protocol/Internet Protocol or TCP/IP and includes future versions thereof. See s 1 of the Electronic Communications and Transactions Act 25 of 2002 (ECT Act). In simple terms, it is "that medium through which your e-mail is delivered and web pages get published". See Lessig

cyber-stalking and cyber-bullying. The insufficiency of the law to deal with novel ICT consternations can be revealed after examining certain related aspects of Chapter XIII of the Electronic Communications and Transactions Act (ECT Act).[20] This chapter states, *inter alia*, that a person or computer user is guilty of an offence if he or she accesses[21] or interferes with data[22] without having obtained the required authority to do so.[23] Thus, the limitation of Chapter XIII of the ECT Act is associated with its inability to address the conventional ways of accessing or interfering with data. For example, modern criminals do not necessarily need to be connected to a computer in order to access or interfere with data wrongfully. Any device or gadget that can be connected to the Internet can be used to access and interfere with data. Therefore, although Chapter XIII of the ECT Act may have dealt adequately with cases relating to the unauthorised accessing of data at the time that the ECT Act was passed, this may not be true as regards controlling the novel and future ways of accessing and interfering with data. This is because the reach that criminals currently have in being able to access personal information[24] stored online is incomparable to that which is envisaged by the ECT Act. Consequently, the latter chapter does not seem to recognise that the Internet[25] (or its future iterations) will generate additional openings for criminals to access and interfere with data using unconventional means.

The shortcomings of law as an ICT regulatory mechanism have to do with the limitations of human conduct in general. Particularly, they are a product of what Dewey refers to as the "blind hunch".[26] This blind hunch exists in situations where human beings act "not upon deliberation, but from routine, instinct, the direct pressure of appetite."[27] ICT regulators rely on blind hunch to regulate ICTs, using common sense; and sometimes they withhold reasons for the chosen regulations fearing that they may be illegitimate. An example of such a hunch, in the South African context, is found in the Electronic Communication and Transactions Amendment Bill, 2012. The Bill seeks, among other things, to supplement the ECT Act. However, it fails to do this. Instead, it compounds the existing ICT regulatory challenges by creating a multitude of what are to be considered "e-crimes" in the future. Some of these so-called e-crimes do not make sense to an ordinary

*Code: Version 2.0* (2006) 9. On the other hand, the word "Web" is defined in s 1 of the ECT Act as an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer.

20 25 of 2002.

21 In terms of s 85 of the ECT Act, the term "access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

22 Data refers to the electronic representations of information in any form. See s 1 of the ECT Act.

23 See ss 86 and 87 of the ECT Act. See also s 119 read with ss 124 and 125 of the Ghanaian Electronic Transactions Act 777 of 2008.

24 For a definition of the term "personal information", see s 1 of the ECT Act.

25 The term "Internet" is defined in s 1 of the ECT Act as the interconnected system of networks that connects computers around the world using the TCT/IP and includes future versions thereof.

26 Dewey "Logical Method and Law" 1924 33 *The Philosophical Review* 560 560.

27 Dewey 1924 *The Philosophical Review* 560.

computer user. Specifically, e-crimes may hinder some important aspects of ICT – for example, availability, neutrality and privacy.

Therefore, an ICT regulatory approach that is external to the law is examined. This approach is abstracted from regulations and accepts that regulations, as opposed to legal rules, are flexible.[28] Particularly, regulations do not require a stringent following of the law-making process. Furthermore, the approach provides for an amorphous controlling framework that is or can be applied to any widely derived source of control or direction.[29] In investigating the ICT regulatory approach modelled from regulations, this article is divided into a number of sections. The second section studies the current debate regarding the ICT regulatory process. In particular, it exposes the opposing views as to whether it is possible to regulate recent technologies. The third section investigates some of the theories[30] for this regulation. The fourth section discusses the possible structure for ICT regulations. This suggested structure is founded on some of the existing principles of regulation. The last section of the article is the conclusion, comprising a general summary of the facts and a recommended way forward for the meaning and structure of ICT regulations in South Africa.

## 2 ICT REGULATORY DEBATE

This section examines the existing debate regarding the ICT regulatory process. In particular, it exposes the opposing views on whether it is possible to regulate recent technologies. The question regarding whether or not it is possible to regulate (or govern) ICTs has been the subject of academic scrutiny for many years.[31] There are some who argue that these technologies are impossible to regulate.[32] They base this claim on the fact that ICTs possess or create their own spaces.[33] This space is referred to as "cyberspace".[34] Cyberspace is described as a space where no one is in charge. Simply put, it is a computer-generated condition having the look and feel of the physical world.[35] A computer user is attracted into this space by its radiance, efficiency and effectiveness.[36] When people relocate to cyberspace, they become free from offline or state command and control.[37] In this context, cyberspace becomes a "mysterious conglomeration of virtual

---

28 Stenning, Shearing, Addario and Condon "Controlling Interests: Two Conceptions of Order in Regulating a Financial Market" in Friedland (ed) *Securing Compliance: Seven Case Studies* (1990) 88 102.

29 Murray "Conceptualising the Post-Regulatory (Cyber) State" in Brownsword and Yeung (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (2008) 287 288.

30 For purposes of this article, the term theory means "a set of propositions or hypothesis about why regulations or regulatory processes emerge, which actors contribute to that emergence and typical patterns of integration between regulatory actors".

31 See Weber *Shaping Internet Governance: Regulatory Challenges* (2009) 203.

32 Johnson and Post "Law and Borders: The Rise of Law in Cyberspace" 1996 48 *Stanford Law Review* 1366 1379.

33 Johnson and Post 1996 *Stanford Law Review* 1379.

34 Murray in Brownsword and Yeung *Regulating Technologies* 300.

35 Gibson *Neuromancer* (1984) 16.

36 Lessig *Code: Version 2.0* 9.

37 Lessig *Code and Other Laws of Cyberspace* (1999) 135.

communities"[38] and a "lawless frontier where anarchy and vigilantism are alive and well".[39] In this space, regulations

> "[a]dapt by continuous increments and at pace second to geology in its stateliness. Technology advances in ... lunging jerks like punctuation of biological evolution grotesquely accelerated ... this Mismatch is permanent".[40]

On the basis of the discussion made above, technology and regulations become adversaries. Technology represents contemporary undertakings and innovation.[41] This does not imply that technology is separate or even more significant in society than other innovative imperatives – for example, science. It simply signifies that technology innovation augments the development of the qualities of a society. In other words, it facilitates growth and expansion. This development normally occurs without technology being tied to a particular jurisdiction or regulations. However, regulations signify command, bureaucracy and an affront to development.[42] In other words, they assume the undertones of legal positivism – that is, they become a set of legal rules that determine when they should be imposed on those not obeying a particular command.[43]

In addition, there are those who discard the supposed individuality of cyberspace.[44] They state that cyberspace is related to the physical space.[45] Specifically, the activities that are carried out through the use of technologies have importance to the computer users or other entities that rely on computers.[46] For example, suppose that Mike is a client of Brown Bank. Mike wishes to access Brown Bank's Internet banking (e-banking) facilities in order to transfer money to Clara. In terms of Brown Bank's e-banking facilities, all its customers must punch in their identifying details (pin, password or code) before they can log in to Brown Bank's e-banking facilities. Accordingly, Mike has to comply with the regulations of his resident country, of the country where Brown Bank's computers are located, and of the country where Brown Bank is physically situated. These regulations are, *inter alia*, those that relate to the privacy and protection of national borders. Once logged in to Brown Bank's e-banking facilities, Mike has to comply with the regulations that are created for and by cyberspace. These include those that regulate the manner of processing and sharing information online,

---

38 These communities are referred to as the "persistent, interactive, simulated social places where (computer) users employ avatars". See Castronova *Synthetic Worlds: The Business and Culture of Online Games* (2005) 287.

39 Biegel *Beyond Our Control? Confronting the Limits of Our Legal Systems in the Age of Cyberspace* (2003) 1–2.

40 Barlow http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/idea_economy_article.html.

41 Wiener "The Regulation of Technology, and the Technology of Regulation" 2004 26 *Journal of Technology in Society* 483 483.

42 Wiener 2004 *Journal of Technology in Society* 483. See also Raymond *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolution* (1999) 55–61.

43 Eastbrook "Cyberspace and the Law of the Horse" 1996 *University of Chicago Legal Forum* 207 209.

44 See Kerr "The Problem of Perspective in Internet Law" 2003 91 *Georgetown Law Journal* 357 362–363. See also Weber *Shaping Internet Governance: Regulatory Challenges* 3–4 and Bonnici *Self-Regulation in Cyberspace* (2008) 1.

45 Weber *Shaping Internet Governance: Regulatory Challenges* 3–4.

46 Bonnici *Self-Regulation in Cyberspace* 1.

encryption and e-authentication.[47] With this in mind, it is submitted that ICT regulation is not a phenomenon or process completely disconnected from real or physical space. Specifically, an activity undertaken through the use of these technologies has an impact on other activities that occur in non-virtual spaces. Accordingly, cyberspace is a space or sphere where regulations apply or should apply.

This article takes the view that ICTs can be regulated. Specifically, it accepts that regulating an ever-changing phenomenon like ICTs is always cumbersome. Every technological innovation (such as steam energy, magnetic or electronic forces, steel, electricity and chemicals, computers and the Internet) requires a society to adjust to contemporary developments. The question then is how to regulate these technologies. ICT regulatory structures may vary from country to country. For example, Germany is examining ways of developing strict liability principles, founded in or to be deduced from the law of contract, to deal with developments associated with the Fourth Industrial Revolution.[48] This is because big or massive data is constantly used in concluding contracts online. However, there may be a point where consensus is reached regarding the proper regulatory scheme to be followed.

In this regard, it is helpful to consider a number of theories for ICT regulations. These theories are not ICT regulations as such. They simply assist in establishing suitable ICT regulations.[49] The theories discussed in this article are the codes-based theory, the danger or AIS theory, the systems theory and the good regulator theorem.

## 3 SELECTED ICT REGULATORY THEORIES

This section studies theories for ICT regulation. It is essential to note that these theories are not necessarily law or regulations. They simply assist in establishing ICT regulations. Specifically, the theories support the creation of a method of ICT regulatory reasoning that is bound to the technologies to be regulated and that is able to progress with them. Such regulatory thinking renounces the idea of re-inventing the ICT regulatory wheel.[50]

### 3 1 Codes-based theory

The codes-based theory found its significance during the 1990s. Some of the prominent proponents of this theory are Reidenberg[51] and Lessig.[52] The

---

47 For a full discussion of how the e-authentication process operates, or should be operated, in South Africa, see Ch VI (Authentication Service Providers) of the ECT Act.

48 Hereinafter referred to as 4IR, which signifies the amalgamation of digital technologies – for example, computers hardware, software and networks, and the manner in which these technologies communicate across the physical, digital and biological domains.

49 For further interesting reading, see McGregor "Law on a Boundless Frontier: The Internet and International Law" 1999 88 *Kentucky Law Journal* 967 969.

50 Susskind *The Future of Law: Facing the Challenges of Information Technology* (1996) 2–43.

51 See Reidenberg "*Lex Informatica:* The Formulation of Information Policy Rules Through Technology" 1998 76 *Texas Law Review* 553.

theory is sometimes compared with techno-regulation.[53] Techno-regulation regards the codes as well as the design of the codes to be important in the regulatory repertoire. Codes refer to computer codes – for example, a password, pin or username.[54] Furthermore, codes refer to the architecture[55] or the technical architecture of the Internet[56] – for example, the hardware and software.[57] In the latter regard, it includes the layers that constitute an information system.[58] These are the content layer (symbols and images), the application layer (underlying infrastructure on which the Internet or Web programmes operate), the transport (TCP) layer, the Internet protocol (IP) layer (infrastructure that handles the flow of data), the link layer (interface between the physical layer and network layer) and the physical layer (copper, wire and links).[59]

The codes-based theory that Reidenberg propagates is called the *lex informatica* and is discussed in the section below. Thereafter, Lessig's theory of regulation by codes or "code is law" is investigated.

### *3 1 1 Lex informatica*

*Lex informatica* is inspired by the work of the Law Merchant (*lex mercatoria*) of the Middle Ages.[60] The Law Merchant was simply the law of diverse nations.[61] This law was drawn from the practices and customs of these nations.[62] It regulated issues relating to cross-border trading[63] and was

---

52 See generally Lessig *Code and Other Laws of Cyberspace*, and Lessig "The Path of Cyberlaw" 1995 104 *The Yale Law Journal* 17–46.

53 Brownsword "What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity" in *Global Governance and the Quest for Justice* (2005) 203 203–206.

54 Koops "Criteria for Normative Technology: The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values" in Brownsword and Yeung *Regulating Technologies* 157 158.

55 Lessig *Code and Other Laws of Cyberspace* 134.

56 Bonnici *Self-Regulation in Cyberspace* 115.

57 Kesan and Shah "Deconstruction Code" 2003 *Yale Journal of Law and Technology* 281. It is essential to note that the distinction between hardware and software is important for ICT regulatory purposes. Grübler provides that hardware involves a collection of tools that enhance the ability of a person to do a job. See Grübler *Technology and Global Change* (1998) 20. Software refers to the (non-human elements of) systems or codes that propel a technology to operate in a particular manner. See Arageorgis and Baltas 1989 *Zeitschrift für Allgemeine Wissenschaftstheorie* 212 212.

58 An information system is a system for generating, sending, receiving, storing, displaying or otherwise processing data messages (data that is generated, sent, received or stored by electronic means, and includes a voice, where the voice is used in an automated transaction – that is, an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment; and a stored record) and includes the Internet. See s 1 of the ECT Act.

59 See Chung and Solum "The Layers Principle: Internet Architecture and the Law" 2004 79 *Notre Dame Law Review* 815.

60 Johnson and Post 1996 *Stanford Law Review* 1389.

61 Pollock and Maitland *The History of English Law Before the Time of Edward I* 2ed (1968) 467; Trakman "From the Medieval Law Merchant to E-Merchant Law" 2003 53 *University of Toronto Law Journal* 265 265.

62 Trakman 2003 *University of Toronto Law Journal* 265.

abstracted from the merchant rules applied by special merchant courts.[64] Given the success of these rules in regulating issues of trade, Reidenberg developed what he referred to as the *lex informatica*. The *lex informatica* examines the differences between the law and the technical architecture of the Internet. The *lex informatica* recognises that legal rules operate differently from technological rules. This divergence lies in the structures that form the basis of these rules. For example, Reidenberg argues that the rudimentary structure for legal regulation is the law,[65] while the foundation for the *lex informatica* is the Internet as an architecture – that is, the HTTP and the default rules.[66] He further argues that the basis for legal rules is the State or government,[67] while the foundation for the *lex informatica* is the technology developer and the social process in terms of which the use of the technology develops.[68]

Accordingly, Reidenberg submits that technologies generally impose regulations on computer users.[69] The structure of these technologies – that is, the design choices – requires compliance with these rules. Therefore, ICTs are regulated through or by reference to their design choices.[70] The latter arises because the manner in which they are designed determines who may access these technologies and who should not.[71] This access depends on whether a person – namely, a computer user – holds the required key, such as a username or password.

### *3 1 2 Code is law*

This theory builds on or is an extension of the *lex informatica*. It accepts that there is a separation between physical space and cyberspace. The notion of "dual presence" is introduced in order to illustrate this difference. The latter indicates that computer users generally occupy two spaces at once. They are both offline and online at the same time. Because of this dual presence, computer users communicate and transact online in ways not known or possible in physical spaces.[72] More specifically, computer users

> "[m]eet, and talk, and live in cyberspace in ways not possible in real space. They build and define themselves in cyberspace in ways not possible in real space. And before they get cut apart by regulation, we should know something about their form, and more about their potential".[73]

---

63 Benson "It Takes Two Invisible Hands to Make a Market: *Lex Mercatoria* (Law Merchant) Always Emerges to Facilitate Emerging Market Activity" 2010 3 *Studies in Emerging Order* 100 101; Kerr "The Origin and Development of the Law Merchant" 1929 15 *Virginia Law Review* 350.

64 Mefford "*Lex Informatica*: Foundations of Law on the Internet" 1997 5 *Indiana Journal of Global Legal Studies* 211 223–224.

65 Reidenberg 1998 *Texas Law Review* 566–567.

66 *Ibid.*

67 *Ibid.*

68 *Ibid.*

69 Murray *The Regulation of the Internet: Control in the Online Environment* (2007) 8 and Paré *Internet Governance in Transition: Who is the Master of This Domain?* (2003) 54.

70 Ong *Mobile Communication and the Protection of Children* (2010).

71 Paré *Internet Governance in Transition* 54.

72 Lessig 1995 *The Yale Law Journal* 17–46.

73 *Ibid*.

In real spaces, legal rules regulate and constrain the manner in which computer users communicate and transact. Examples include copyright laws, defamation laws, online child pornography laws, and cyberstalking laws.[74] However, codes regulate the manner in which computer users communicate and transact in cyberspace.[75] One example of online regulation is the software known as Internet filtering, which prevents or limits access to and distribution of particular data.[76] It is clear that the interaction between legal rules and the technical structures of ICTs is essential for ICT regulations.

## 3 2 Danger or AIS theory

The danger theory is inspired by biology. It is motivated by the workings of the biological immune system (BIS).[77] For example, the BIS has a number of cells or molecules or lymphocytes, macrophages, dendritic cells, natural killer cells, mast cells, interleukins and interferons.[78] It is a defence organism or mechanism for the human or organic body.[79] This defence is provided against certain unknown or external attacks (pathogens).[80] These attacks can be in the form of bacteria and viruses.[81] Generally, the BIS distinguishes and discriminates between known or self-attacks and unknown or non-self-attacks.[82] For these attacks to be recognised by a system, alarm signals (pattern recognition receptors) from injured tissues are reported.[83] Subsequently, the immune system reacts by breaking down these attacks. It does all this in order to restore a balance in the body.[84] In cases where a balance could not be maintained, the immune system collapses and it subsequently becomes necessary to immunise the system with needed security-improving or enrichment measures.

---

74 Lessig "Law Regulating Code Regulating Law" 2003 35 *Loyola University Chicago Law Journal* 1 1.

75 Lessig *Code: Version 2.0* 88. See also, Grimmelmann "Regulation by Software" 2005 114 *The Yale Law Journal* 1719 1721.

76 McIntyre and Scott "Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility" in Brownsword and Yeung *Regulating Technologies* 109.

77 Lee, Kim and Hong "Biologically Inspired Computer Virus Detection System" in Ijspeert, Murata and Wakamiya (eds) *Biologically Inspired Approaches to Advanced Information Technology* (2004) 153 155.

78 Hofmeyr and Forrest "Immunity by Design: An Artificial Immune System" in *Genetic and Evolutionary Computation* (papers presented at the Genetic and Evolutionary Computation Conference (GECCO-99) Orlando Florida 1999) 1289 1290.

79 Rowe *Theoretical Models in Biology: The Origin of Life, the Immune System and the Brain* (1994) 121.

80 Rowe *Theoretical Models in Biology* 121.

81 *Ibid*.

82 Matzinger "The Danger Model: A Renewed Sense of Self" 2002 296 *Science* 301 301. For an interesting study of self-non-self-attacks, see Bretscher and Cohn "A Theory of Self-Non-Self-Discrimination" 1970 169 *Science* 1042 1042–1046.

83 Matzinger 2002 *Science* 301.

84 *Ibid*.

The artificial immune system (AIS) theory argues that a biological body can be understood in terms of codes, dispersals or networks.[85] These codes are robust, adaptable and autonomous,[86] making for similarities between the workings of a human body and that of a computer.[87] Computers are dynamic, in that programmes and software are installed and erased whenever needed, new computer users emerge regularly, and configurations always change.[88] The danger theory proposes that computers be built with self-protective codes analogous to the BIS. The system has to be able to respond to self and non-self-attacks. These attacks must be measured by "damage to cells indicated by distress signals that are sent out when cells die an unnatural death (cell stress or lytic cell death, as opposed to programmed cell death or *apoptosis*)".[89] A set of detectors – that is, an intrusion detection system – has to be built within the system. These detectors should identify anomalies in a system.[90] Thereafter, the anomalies have to be matched with known or probed intrusions. In cases where a match is established, the detectors must be automatically activated.[91] This activation has to lead to a process whereby a report is sent to an operator or administrator of a system who must then assess the anomalies and take appropriate action.[92]

## 3 3 Systems theory

Ludwig Von Bertalanffy introduced the systems theory in the 1930s. For Von Bertalanffy, an examination of systems has been a province for academic scrutiny over many years. However, academics have omitted to investigate the dynamics of systems. Because of this omission, Von Bertalanffy presented the idea of a General System Theory,[93] which starts from the premise that "every living organism is an open system, characterised by a continuous import and export of substances or subsystems".[94] Therefore, systems are elements of an operated organism.[95] Such an organism is referred to as the whole or wholeness of a system; a computer is an

---

85 Birke *Feminism and the Biological Body* (1999) 142 and Dasgupta, Yu and Nino "Recent Advances in Artificial Immune Systems: Models and Applications" 2011 1 *Applied Soft Computing* 1574 1574–1575.

86 Hofmeyr and Forrest "Architecture for an Artificial Immune System" 1999 7 *Evolutionary Computation* 45–68 45.

87 Hofmeyr and Forrest 1999 *Evolutionary Computation* 46.

88 *Ibid*.

89 Aickelin and Cayzer "The Danger Theory and its Application to Artificial Immune Systems" (papers delivered at the 1st Intentional Conference on Artificial Immune Systems (ICARIS-2002), 2002 Canterbury) 141 141.

90 Aickelin, Bentley, Cayzer, Kim and Mcleod "Danger Theory: The Link Between AIS and IDS?" in Timmis, Bentley and Hart (eds) *Artificial Immune Systems* (2003) 147 147–148.

91 Aickelin *et al* in Timmis, Bentley and Hart *Artificial Immune Systems* 148–149.

92 Aickelin *et al* in Timmis, Bentley and Hart *Artificial Immune Systems* 150.

93 See Von Bertalanffy *General System Theory: Foundations, Development, Applications* (1968) and Von Bertalanffy *Perspectives on General System Theory: Scientific-Philosophical Studies* (1975).

94 Von Bertalanffy *Perspectives on General System Theory* 38.

95 Von Bertalanffy *Perspectives on General System Theory* 159.

example.[96] The aforesaid organism includes a "set of social, biological, technological or material partners that collaborate on a common purpose".[97]

For the sake of completeness, the idea of computers operating like living organisms requires clarification. This idea does not necessarily advocate that computers have a life of their own, nor does it imply that computers operate in a manner as described in Plato's two-world theory – namely, the sensible and intelligible worlds.[98] Specifically, computers carry out functions as directed by computer users. These tasks are usually beyond the scope of what is normally anticipated in offline spaces. In other words, computers fall within the category of objects that could be referred to as artificial or man-made things.[99] The latter are products generated by art rather than nature and do not have relations with the essence of matter – for example, the force of gravity.[100]

For ICT regulatory purposes, the theory by Von Bertalanffy argues that systems produce their own existence within a living organism.[101] They cultivate their own languages. These languages are appropriately understood by those who habitually or consistently work with the living organism. The latter include technicians or computer programmers,[102] but do not include, what Von Bertalanffy refers to as, computer morons, button-pushers or learned idiots[103] – that is, those who do not contribute to computer innovation and to solving prevailing technology regulatory challenges.[104]

Consequently, Von Bertalanffy submits that any framework to regulate ICTs should involve a suitable examination of the whole or wholeness of the systems that constitute the living organism.[105] This scrutiny requires or compels ICT regulators to study the elements of the living organism and comprehend the manner in which these elements operate, both exclusively and together.

## 3 4 Good regulator theorem

Conant and Ashby support the good regulator theorem.[106] They postulate that every good regulator of any arrangement must be a reproduction of that

---

96 Von Bertalanffy *General System Theory* 5; Von Bertalanffy *Perspectives on General System Theory* 157.

97 Febbrajo "The Rules of the Game in the Welfare State" in Teubner (ed) *Dilemmas of Law in the Welfare State* (1986) 129.

98 Huard *Plato's Political Philosophy: The Cave* (2007) 35–37. See also Solomon and Higgins *The Big Questions: A Short Introduction to Philosophy* 8ed (2010) 121–123.

99 Simon *The Sciences of the Artificial* 3ed (1996) 3–5.

100 Simon *The Sciences of the Artificial* 4.

101 Samuelson "Five Challenges for Regulating the Global Information Society" in Marsden (ed) *Regulating the Global Information Society* (2000) 317.

102 Von Bertalanffy *General System Theory* 10.

103 *Ibid*.

104 *Ibid*.

105 Von Bertalanffy *Perspectives on General System Theory* 157.

106 See in general Conant and Ashby "Every Good Regulator of a System Must Be a Model of That System" 1970 1 *International Journal of Systems Science* 89. See also Scholten "A Primer for Conant & Ashby's Good-Regulator Theorem" http://www.goodregulatorproject.

specific arrangement.[107] An agenda to regulate ICTs must accordingly be a representation of the hardware and software that is elementary to the technology to be regulated.[108] This view is best captured by the notion that "every good key must be a model of a lock it opens".[109] Simply put:

> "The *pursuit* of a goal by some dynamic agent in the face of a source of obstacles places at least one particular and unavoidable *demand* on that agent, which is that the agent's behaviours *must* be executed in such reliable and predictable way that they can serve as a *representation* of that source of obstacles".[110]

It has to be remembered that ICTs are a mishmash of systems and networks, many of which have sub-systems and sub-networks. The systems and networks have similar appearances and these appearances have similar structures. For ICT regulatory purposes, regulators should develop regulatory models that appreciate the functioning or non-functioning of the systems and networks. The rationale ought to be to establish a regulatory agenda that not only controls existing hindrances, but also is able to provide solutions to potential disputes.[111] This agenda has to discourage regulators from invariably re-inventing the technology regulatory wheel.[112] Instead, regulators must anticipate the workings of a system or network.[113] Subsequently, they must create regulations that are bound to the technology to be regulated and are able to evolve with it.[114]

## 3 5 From theory to ICT regulation

In the sections above, it was stated that a better way to study ICT regulations is to look outside or beyond legal rules. This is the position because legal rules are inflexible and follow an elongated process. It was therefore surmised that certain ICT theories could provide a basis for an ICT regulatory structure that is external to legal rules. The next section examines an ICT structure that is gleaned from the ICT regulatory theories discussed above. It postulates a number of role-players for ICT regulation. Particularly, it recognises that these role-players can, in the process of regulating ICTs, elect a particular ICT regulatory agenda. This agenda can be extrapolated from the manner and form of the technology to be regulated. In this manner, the law or legal rules only play a persuasive function.

---

org/images/A_Primer_For_Conant_And_Ashby_s_Good-Regulator_Theorem.pdf (accessed 2016-11-18).

107 Conant and Ashby 1970 *International Journal of Systems Science* 89.

108 Murray in Brownsword and Yeung *Regulating Technologies* 290.

109 Scholten "Every Good Key Must Be a Model of the Lock it Opens – (The Conant and Ashby Theorem revisited)" http://www.goodregulatorproject.org/images/Every_Good_Key_Must_Be_A_Model _Of_The_Lock_It_Opens.pdf. (accessed 2020-01-16).

110 *Ibid*.

111 Susskind *The Future of Law* 2–43.

112 Brownsword "So What Does the World Need Now? Reflections on Regulating Technologies" in Brownsword and Yeung *Regulating Technologies* 23 30.

113 Forrester "Industrial Dynamics: A Major Breakthrough for Decision Makers" 1958 36 *Harvard Business Review* 37 37.

114 Brownsword *Reflections on Regulating Technologies* 27.

# 4 ICT REGULATORY STRUCTURE

## 4 1 Overview

Generally, developing flawless regulations is almost impossible. There will always be some who seek ways to bypass ICT systems (computer hardware, software, Internet, data or computer applications) and thus create loopholes in regulations. A proper understanding here requires one to separate so-called real programmers from computer crackers. Real programmers are computer experts who assiduously test and evaluate the security of ICT systems.[115] Because these programmers have to do with Open-Source Development, they design hacking attacks and launch those attacks against a system.[116] The intention is to ensure that the system is secure before it is rolled out to the general public. In contrast, computer crackers use nefarious means to compromise and gain entry into ICT systems;[117] the crackers alter, access or retrieve information belonging to another person without the latter's consent. Therefore, ICT regulations seek to alleviate the extent of the risks to which ICTs may be exposed through computer cracking.

To improve ICT regulations, it is argued that a decentring analysis of regulations can provide suitable solutions to the regulatory agenda. In this way, regulations become a product of diverse role-players. These could be the State and the regulated industries – for example, society, communities, private and public institutions and computer users. The purpose is to establish Better (ICT) Regulations.[118] These regulations have everything to do with promoting Good ICT Regulations.[119] Good Regulations imply that for every ICT regulatory framework ICT regulations conform to specific standards.[120] These are that: a legislative authority should support the regulations; there has to be a suitable structure for accountability; the regulatory structure ought to be reasonable, accessible and open; and ICT regulators have to possess the necessary skills and expertise.[121]

In the aforementioned regard, regulatory role-players have to determine the standards to be applied in each case. In doing so, they can elect an agenda based on smart regulations, self-regulation, meta- or reflexive regulations, or co-regulations.[122]

---

115 Raymond *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolution* (2001) 3–4.

116 Bossler and Burruss "The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?" in Holt and Schell (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (2011) 38 40.

117 S 86(1)–(2) of the ECT Act.

118 Gunningham "Enforcement and Compliance Strategies" in Baldwin, Cave and Lodge (eds) *The Oxford Handbook of Regulation* 120 131. Better ICT Regulations are the opposite of "Less ICT Regulations". See Kirkpatrick and Parker "Regulatory Impact Assessment: An Overview" in *Regulatory Impact Assessment: Towards Better Regulation* (2007) 1 1–2.

119 Baldwin and Cave *Understanding Regulation* 76.

120 *Ibid*.

121 *Ibid*.

122 See Baldwin "Better Regulation in Troubled Times" 2006 1 *Health Economics, Policy and Law* 203.

## 4 2 ICT regulatory agenda

### *4 2 1 Smart regulations*

Smart regulations are distinguished from dumb regulations. Dumb regulations demonstrate themselves in countless ways. They place pointless burdens on businesses and they fail to reflect changing technology. To put it bluntly, Flemming argues that dumb regulations leave "investors as sheep to be sheared".[123] However, smart regulations support development outside of government rules.[124] They provide the basis for the view that legal rules are usually unsatisfactory in controlling social behaviour.[125] In other words, smart regulations generally accept the existence of a variety of regulatory methods outside of the command-and-control way of regulating; thus, smart regulations provide a flexible, imaginative and innovative form of social control. For this reason, the Organisation for Economic Co-operation and Development (OECD) stipulates that these regulations signify a shift away from unnecessary regulatory red tape to a smart and simplified regulatory process. This is because smart regulations encourage management of the role of the State, business and individual computer users.[126] This normally occurs because these regulations require a suitable examination of legal rules and the normative standards that are set by these rules.[127]

In practice, the consumer and environmental fields remain examples of areas where smart regulations are applied. For example, the European Consumer Organisation (the BEUC)[128] articulates the need for smart regulations.[129] It acknowledges that this form of regulating is crucial because it places the welfare of consumers at the forefront of the regulatory process.[130] In turn, the OECD developed the document *From Red Tape to*

---

123 Flemming "The Importance of Smart Regulation" https://www.sec.gov/news/speech/importance-of-smart-regulation.html (accessed 2016-03-13).

124 House of Commons Regulatory Reform Committee *Getting Results: The Better Regulation Executive and the Impact of the Regulatory Reform Agenda* (2008) 181–184 and Gunningham "Regulating Biotechnology: Lessons from Environmental Policy" in Somsen (ed) *The Regulatory Challenge of Biotechnology: Human Genetics, Food and Patents* (2007) 3 6.

125 House of Commons Regulatory Reform Committee *Getting Results* 181–184.

126 Gunningham and Sinclair "Designing Principles for Smart Regulations" in Ramesh and Howlett (eds) *Deregulation and its Discontents: Rewriting the Rules in Asia* (2006) 195 195–196.

127 European Commission "Smart Regulation in the European Union" (8 October 2010) http://ec.europa.eu/smart-regulation/ (accessed 2015-05-13) 2–3.

128 The BEUC is an umbrella group that was founded in 1962. It investigates European Union (EU) decisions and developments that are likely to affect consumers. It does all this by focussing on its five main priorities – that is, financial services, food, digital rights, consumer rights and enforcement and sustainability. See European Consumer Organisation (BEUC) http://www.beuc.eu/about-beuc/who-we-are (accessed 2016-11-21).

129 European Consumer Organisation "Smart Regulation: BEUC Response to the Stakeholder Consultation" http://ec.europa.eu/smart-regulation/consultation_2012/docs/registered_organisations/beuc_en.pdf (accessed 2016-03-13).

130 European Consumer Organisation http://ec.europa.eu/smart-regulation/consultation_2012/docs/registered_organisations/beuc_en.pdf.

*Smart Tape: Administrative Simplification in OECD Countries*,[131] which argues for a flexible and ICT-driven self-regulatory system that should, in general, reduce the administrative burden (red tape) associated with regulations.[132] In addition, such a system should promote innovation, trade, investment and economic efficiency (smart tape).[133] In this article, these are referred to as smart regulations.

### *4 2 2 Self-regulation*

Self-regulation basically implies self-control and self-correction[134] and is a significant human quality. For example, Zimmerman illustrates this understanding by stating:

> "Perhaps our most important quality as humans is our capacity to self-regulate. It has provided us with an adaptive edge that enabled our ancestors to survive and flourish when changing conditions led other species to extinction. Our regulatory skill or lack thereof is the source of our perception of personal urgency that lies at the core of our sense of self."[135]

Following this passage, Zimmerman defines self-regulation as "self-generated thoughts, feelings, and actions that are planned and cyclically adapted to the attainment of personal goals".[136] In terms of this definition, there are multiple traits, abilities or stages of competencies necessary for self-regulation. For example, regulatory role-players regulate their activities or affairs in order for those activities and affairs to be in line with certain anticipated ends.[137] The triadic understanding of self-regulation – that is, personal, behavioural and environmental processes – informs the achievement of these ends. Specifically, it determines how the regulatory role-players interact with each other in a manner that establishes a set of regulatory standards for their compliance.[138]

Schraw, Crippen and Hartley argue that self-regulation is fundamental in science education.[139] From the forgoing, regulators identify the intended regulatory objectives and eliminate certain factors that prevent or are likely

---

131 See OECD *From Red Tape to Smart Tape: Administrative Simplification in OECD Countries* (2003).

132 OECD *From Red Tape to Smart Tape* 5.

133 OECD *From Red Tape to Smart Tape* 8.

134 Carver and Scheier "Self-Regulation of Action and Affect" in Vohs and Baumeister (eds) *Handbook of Self-Regulation, Second Edition: Research, Theory, and Applications* (2011) 3 3–4.

135 Zimmerman "Attaining Self-Regulation: A Social Cognitive Perspective" in Boekaerts, Pintrich and Zeidner (eds) *Handbook of Self-Regulations* (2000) 13 13.

136 Zimmerman in Boekaerts, Pintrich and Zeidner *Handbook of Self-Regulations* 13.

137 Hrabok and Kerns "The Development of Self-Regulation: A Neuropsychological Perspective" in Solok, Müller, Carpendale, Young and Larocci (eds) *Self and Social Regulation: Social Interaction and the Development of Social Understanding and Executive Functions* (2010) 129 129.

138 Bonnici *Self-Regulation in Cyberspace* 10.

139 See in general Schraw, Crippen and Hartley "Promoting Self-Regulation in Science Education: Metacognition as Part of a Broader Perspective on Learning" 2006 36 *Research in Science Education* 111.

to prevent the goals from being achieved.[140] In order to do this, the regulators select strategies that assist in achieving the identified goals, implement those strategies, and monitor the progress towards the attainment of the goals.[141] This process is not simply a box-ticking exercise. However, it is an involving process that requires a proper understanding of and engagement with the regulations, and the scheme to be regulated. For example, the triad underpinning self-regulation and how it relates to the regulatory process or process is essential.

### *4 2 3 Meta-regulations*

Meta-regulations are also called reflexive regulations because "meta", in the sense in which it is used, posits some form of flexibility that cannot be ascribed to self-regulation.[142] Essentially, this flexibility is such that it becomes accepted that

> "[f]ormal rules are based on the principles, not prescription, to allow for the necessary flexibility in regulatory practice; law (the regulator) is reflexive and responsive (although this means different things in the detail), in order to learn about what works to meet the public interest and to include relevant stakeholders in regulatory processes ... Third parties such as non-governmental organisations and activists support regulation by acting as civil regulators, providing further relief for regulatory resources as well as reducing the chance of regulatory capture by industry."[143]

Therefore, reflexive regulations, which are the domain of reflexive governance,[144] provide a structure to control other associated regulatory structures.[145] In this manner, reflexive regulations discourage the traditional view of the State as the primary role-player in ICT regulations.[146] For example, the regulator (usually the State) observes how role-players to self-regulations regulate themselves. It (the regulator) only comes to the fore in situations where a self-regulatory breach is identified. For this reason, the capacity of the regulator to conceptualise regulations declines dramatically.[147]

---

[140] Schraw, Crippen and Hartley 2006 *Research in Science Education* 111. See also Leventhal, Brissette and Leventhal "The Common-Sense Model of Self-Regulation of Health and Illness" in Cameron and Leventhal (eds) *The Self-Regulation of Health and Illness Behaviour* (2003) 42 43.

[141] Schraw, Crippen and Hartley 2006 *Research in Science Education* 111.

[142] Simon *Meta-Regulation in Practice: Beyond Normative Views of Morality and Rationality* (2017) 3.

[143] Simon *Meta-Regulation in Practice* 3.

[144] This implies the conditions to ensure the collective maximisation of certain normative or regulatory expectations. See Lenoble and Maesschalck "Renewing the Theory of Public Interest: The Quest for a Reflexive and Learning-Based Approach to Governance" in De Schutter and Lenoble (eds) *Reflexive Governance: Redefining the Public Interest in a Pluralistic World* (2010) 3 3–4.

[145] Levi-Faur "Regulation and Regulatory Governance" in Levi-Faur (ed) *Handbook on the Politics of Regulation* (2011) 3 11.

[146] Lee "In the Prison of the Mind: Punishment, Social Order, Self-Regulation" in Saral, Douglas and Umphrey (eds) *Law as Punishment or Law as Regulation* (2011) 124–154 127.

[147] Gunningham in Baldwin, Cave and Lodge *The Oxford Handbook of Regulation* 8.

The association of meta-regulations with reflexive regulations seems sensible. For example, Morgan argues that meta-regulations "capture[ ] a desire to think reflexively about regulation, such that rather than regulating social and individual action directly, the process of regulation itself becomes regulated".[148] In this manner, regulations become a support structure for the regulatory role-players in establishing their own systems of control and management.[149] In the process, the role of government becomes about regulating at a distance,[150] and sometimes being an agency within which regulations apply.[151]

Studies in, *inter alia*, environmental sciences provide a useful guide for the application of meta-regulations. In these studies, meta-regulations have been found to be helpful in alleviating the dangers caused by pollution.[152] This success has to do with the fact that the regulatory role-players adopt specific regulatory measures and are also able to assess their own performance in meeting these regulations.[153] In South Africa, for example, this form of regulation seems to be preferred by the Health Professions Council of South Africa (HPCSA).[154]

### *4 2 4 Co-regulation*

Co-regulation refers loosely to co-operative regulation or regulation by co-operation. It signifies the combination of government regulation and self-regulation.[155] In this instance, government and self-regulatory industries collaborate in order to establish a particular regulatory paradigm.[156] The government recommends specific regulatory frameworks,[157] and the self-regulatory industries generate principles, methods and ways of administering the government regulations.[158]

The APEC-OECD Integrated Checklist on Regulatory Reform of 2005 issued a policy framework for self-regulation. This framework can be commended given its enunciation of the characteristics for self-regulation (efficiency, transparency and accountability). In terms of this framework, so-called "horizontal criteria concerning regulatory reform"[159] were developed.

---

148 Morgan "The Economisation of Politics: Meta-Regulation as a Form of Nonjudicial Legality" 2003 12 *Journal of Social and Legal Studies* 489 490.

149 Coglianese and Mendelson in Baldwin, Cave and Lodge *The Oxford Handbook of Regulation* 147.

150 Braithwaite "The New Regulatory State and the Transformation of Criminology" 2000 40 *British Journal of Criminology* 222 225.

151 McHarg "Devolution and the Regulatory State: Constraints and Opportunities" in Oliver, Prosser and Rawlings (eds) *The Regulatory State: Constitutional Implications* (2010) 67 80.

152 Gilad "It Runs in the Family: Meta-Regulation and Its Sibling" 2010 4 *Regulation and Governance* 485 491.

153 Gilad 2010 *Regulation and Governance* 491–492.

154 A statutory body established in terms of the Health Professions Act 56 of 1974. See preamble to the Health Professions Act 56 of 1974.

155 Bonnici *Self-Regulation in Cyberspace* 15.

156 *Ibid*.

157 *Ibid*.

158 *Ibid*.

159 Regulatory reform deals with the changes that seek to improve the quality of regulations and augment the economic performance, cost-effectiveness and quality of legal regulations.

These criteria support the idea of integrating policy for regulatory reform in a manner that ensures that the policy is able to deal with other factors – for example, competition and market openness. For example, co-regulations have been found to be productive in the area of food safety.[160] In this field, they are considered to be the most transparent and trustworthy of all regulatory structures.[161] Accordingly, the idea behind co-regulation is to maximise the efficiency, transparency and accountability of the regulations.

## 5 CONCLUSION

The traditional view is that the regulation process is based on the law or legal rules. These rules typically demand that a command-and-control procedure should be followed. In South Africa, the rules to regulate ICTs are contained, *inter alia*, in the ECT Act. The parts of this Act that are important to this article are those that relate to the wrongful or unauthorised accessing and interference with data. The ECT Act governs the conventional ways of accessing and interfering with data. However, it fails to deal with or anticipate future ways of accessing and interfering with information online. Consequently, the ECT Act does not recognise that an evolution of these technologies necessarily brings about contemporary ways of accessing and interfering with information. In other words, the ECT Act ignores the fact that developments in ICTs will mean an expansion of the reach that criminals possess in order to access and interfere with information online.

In this article, the above-mentioned limitations are attributed not only to the ECT Act. Specifically, they also relate to shortcomings in the overall law-making process in South Africa. This has to do with the fact that the law demands compliance with certain established rules. These rules are naturally stagnant and are commonly averse to development. As an alternative response, this article discusses an ICT regulatory approach founded outside of the legal rules. This approach does not necessarily discard the importance of the law in regulating ICTs. Simply, it accepts that regulations, rather than the law, should be flexible. Given the inflexibility of legal rules, legal regulations are likely to prevent a continuous process of regulating in an endeavour to control an evolving phenomenon – namely, ICTs. Such obstruction may be prevented if legal regulations are allowed to assume a facilitative role or function in the sense of channelling the meaning and structure of ICT regulations.

For ICT regulatory purposes, it is submitted that regulations should follow a framework that is different from the one used offline. A suitable understanding of how systems and networks operate is required. This understanding is not a matter of guesswork or ticking boxes. It enjoins regulators – that is, lawmakers and developers of ICTs – to undertake a meaningful study of systems and the dynamics of systems. For example, it

See APEC-OECD "Integrated Checklist on Regulatory Reform" (2005) http://publications.apec.org/Publications/2005/09/APEC-OECD-Integrated-Checklist-on-Regulatory-Reform.

160 Martinez, Fearne, Caswell and Henson "Co-Regulation as a Possible Model for Food Safety Governance: Opportunities for Public–Private Partnerships" 2007 32 *Food Policy* 299 301.

161 Martinez *et al* 2007 *Food Policy* 303–304.

may be necessary to follow the codes-based theory – that is, regulating by means of codes and, thus, "code is law". Furthermore, regulators may adopt the danger theory, wherein regulations are founded on a diligent examination of the systems and networks that form the basis of the technology to be regulated. Such regulations aim to establish ICT regulations that are bound to the technology and are able to develop with it.

Generally, better or good regulations are proposed as the avenue towards achieving the above-mentioned regulatory structure. This means that the ICT regulations must not be a product of a single actor, usually the State. All role-players in the proposed regulatory agenda ought to be involved in the ICT regulatory process. These are, *inter alia*, the State, society, communities, private and public institutions and computer users. To complement this process, the developers of ICTs – that is, the real programmers – ought to be involved in the establishment of ICT regulations. The rationale for this involvement should be to ensure that regulations are not only generated through the mind or skill of the role-players, but also that the role-players take ownership of the said regulations. Consequently, regulators could elect to adopt any or a combination of smart, reflexive, self or co-regulatory structures. The law – that is, the ECT Act – has to be expansive enough to guarantee that this recommended good ICT regulatory framework operates effectively and efficiently.