Disruptive technologies and the future of regulations – ICT regulatory structure(s) determined

Mzukisi N Njontini
LLB LLM LLD
Associate Professor, Faculty of Law, University of Johannesburg

SUMMARY

Digitisation of information compels a revision of the Fourth Industrial Revolution (4IR) and its associated technologies. This arises because 4IR technologies, for example, the Internet of Things (IoT), Big or Massive Data, Artificial intelligence (AI), augmented or virtual reality and machine learning, drastically adjust the manner in which an information society operates. Specifically, they present unprecedented opportunities for business, economy and online user or consumers. Furthermore, they profoundly model and re-model productions. As a result, the conventional lines between the physical, digital and biological spheres become imprecise. Given the extent of the transformation that 4IR technologies bring to society, it has become necessary to refer to them as the disruptive technologies. However, the inquiry is to what extent is the information society ready to take advantage of disruptive technologies and control some of the setbacks that emanate from therefrom? For regulatory purposes, how electronic or e-ready regulators are to control the adverse consequences that are associated with disruptive technologies? To address these questions, this paper discusses some of the selected theories for technology regulations (artificial immune system (AIS) theory and theory for *Lex Informatica*). The theories are not technology regulations, as such. Simply, they concede that technology regulations should encourage a proper scrutiny of the position of the technologies in the information society.

1 Introduction

It has become customary to talk about "disruptive technologies", that is, technologies arising consequent to the Fourth Industrial Revolution (4IR), that have major impact on society.[1] These technologies focus, among others, on the creation of intelligent and communicative systems.[2] These may be systems fostering machine-to-machine (M2M) and human-to-machine (H2M) interactions.[3] When this happens, there is mention of

1 In the information or digital age, reference to a society means the Information Society. See, Webster *Theories of the Information Society* (2002) 2-7.
2 Schwab *Shaping the Future of the Fourth Industrial Revolution: A Guide to Building a Better World* (2018) 23.
3 Schwab *The Fourth Industrial Revolution* (2016) 17.

How to cite: Njontini 'Disruptive technologies and the future of regulations – ICT regulatory structure(s) determined' 2021 *De Jure Law Journal* 174-193
http://dx.doi.org/10.17159/2225-7160/2021/v54a11

technologies, for example, the Internet of Things (IoT),[4] Big or Massive Data,[5] Artificial intelligence (AI),[6] augmented or virtual reality[7] and machine learning.[8] However, one still finds views doubting the effect that 4IR technologies have or continue to have on society. For example, there are those who opine that the idea for disruptive technologies is a fallacy.[9] They argue that all society currently witnesses are mere random technological interruptions.[10] To them, the technological interruptions are not so tumultuous that they revolutionise society or the way society operates. In the main, these assertions are a further development of the idea of "*The Shock of the Old*" established by David Edgerton.[11] This notion propounds that there is no such a thing as radical or extraordinary technologies.[12] Simply, ICTs are products of history.[13] In other words, they emerge, disappear and re-emerge depending on their relevance to society.[14] Because of this, categorising technologies as disruptive is "just a reheated nonsense from a hundred years ago".[15]

As convincing as the view of the Shock of the Old is, it however does not seem to be the most popular amongst academics. Proponents of the 4IR technologies argue that recent technologies present unprecedented opportunities for or paradigm shifts in the economy, business, society,

4 IoT is often referred to as Internet of Everything, Web of Things, Internet of People and Things, Internet of Vehicles, Internet of Animal Health Things and Internet of Services. It is a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) Things based on existing and evolving interoperable information and communication technologies". See, International Telecommunication Union (ITU).

5 Big data is the term used to describe complex or large volumes of data. It really does not matter whether the data is structured, semi-structured or un-structured. It is only sufficient if the data is part of an activity that "collects, analyses, packages, and sells data, even uninteresting-looking data, to reveal tastes, habits, personality, and market behaviour".

6 AI can be defined as machines that have the ability to structure, re-structure, develop itself, and design or re-design more progressive machines. See, Vinge *The Coming Technological Singularity* (1993).

7 Augmented reality implies the real-time direct or indirect view of a physical real-world environment that has been enhanced/augmented by adding virtual computer-generated information to it.

8 Machine learning is also called "automated learning". This is because automation plays a key role to the functioning of the machine. In other words, the AI has the ability to discern, learn and systematise information automatically without the necessity for programming. See, Nagy *Artificial Intelligence and Machine Learning Fundamentals: Develop Real-World Applications Powered by the Latest AI Advances* (2018) 2.

9 Vilakazi "How are Universities Responding to 4IR" in *Proceedings of the 6th DHET Research Colloquium on the Fourth Industrial Revolution (4IR): Implications for Post-School Education and Training* (2019) 15.

10 Vilakazi.

11 See, Edgerton *The Shock of the Old: Technology and Global History Since 1900* (2008).

12 Edgerton xi-xvi.

13 Edgerton xi.

14 Edgerton xvi.

15 Edgerton xvi.

and individual users of these technologies.[16] In other words, ICTs have become so radical that they model and re-model productions, and "blur the lines between the physical, digital and biological spheres".[17] From the business standpoint, these technologies disrupt the manner of generating, creating and preserving value or income.[18] This then creates massive variations in the prevailing models and re-structuring of the data[19] necessary to operationalise businesses. Consequently, questions arise, inter alia, to what extent is society ready to take advantage of 4IR technologies and control some of the setbacks that emanate therefrom? Finding suitable responses to these questions is a challenge to regulators. This ensues because the starting point to commencing legal regulations is usually the adoption of the "command and control" principle.[20] In South Africa, the Cybercrimes and Cybersecurity Bill, 2017 is an example of this challenge.[21] For example, Chapter 2 of this Bill creates more than forty cybercrimes. By so doing, it establishes a framework of over-regulation.[22] In other words, almost all the activities carried out online and without the necessary consent and authority of a person (authorising person) are likely to fall under the category of cybercrimes in terms of this Bill. Commenting on it, the Law Society of South Africa (LSSA) had the following to say:

> "The Cybercrimes and Cybersecurity Bill (the Bill) is a daunting undertaking resulting in a portmanteau of 11 chapters of draft legislation, which include chapters on definitions, offences, jurisdiction, powers to investigate, search

16 Schwab 33-45.

17 Department of Science and Technology White Paper on Science, Technology and Innovation of March 2019 https://www.dst.gov.za/images/2019/WHITE_PAPER_ON_SCIENCE_AND_TECHNOLOGY_web.pdpf (accessed 2020-05-26).

18 Rayna and Striukova "360°Business Model Innovation: Toward an Integrated View of Business Model Innovationa" 2016 *Research Technology Management* 41-51.

19 Data is the electronic representation of information in any form. See, s 1 of the Electronic Communications and Transactions Act 25 of 2002 (hereinafter referred to as the ECT Act).

20 See Baldwin, Cave and Lodge *Understanding Regulation: Theory, Strategy, and Practice* (Oxford 2012) 1-2 and Coglianese and Mendelson "Meta-Regulation and Self-Regulation" in Baldwin, Cave and Lodge (eds) *The Oxford Handbook of Regulation* (2010) 146-168 146.

21 Hereinafter referred to as the Cybercrimes Bill. The object of the Bill is to "create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which are harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; to provide for the establishment of a designated Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations to report cybercrimes; to provide for capacity building; to provide that the Executive may enter into agreements with foreign States to promote measures aimed at the detection, prevention, mitigation and investigation of cybercrimes; to delete and amend provisions of certain laws; and to provide for matters connected therewith". See, Preamble to the Cybercrimes Bill.

22 Njotini *E-Crimes and E-Authentication - A Legal Perspective* (2016) 9.

> and access or seize and international cooperation, 24/7 point of contact, structures to deal with Cybersecurity, National Critical Information infrastructure protection, evidence, general obligations of electronic communications, service providers and liability, agreements with foreign state and so on up to general provisions. From the outset, it is clear that the inclusion of 68 sections in the Bill results in a voluminous document. It is submitted that the unnecessary duplication and incorporation of many common law principles in the Bill has contributed to the 128 pages of draft legislation that is not easy to digest".[23]

For regulatory purposes, the ICT regulatory approach adopted in the Bill is far-reaching and legally unsound and untenable. Specifically, it is abstracted on a framework that is inconsistent with developments in technologies. Furthermore, it offsets the proper application of the Bill and hinders its usefulness to address cybercrimes in South Africa.[24]

Given the challenges mentioned above, some limitations exists with the adopted command and control principles for technology control purposes. Specifically, these shortcomings are unavoidable, especially when regulating a dynamic, energetic and flexible phenomenon similar to the 4IR technologies. Thus, it is necessary to study technologies with particular reference to their position in society. For example, Plato developed what he referred to as the "Two-World Theory" of legal reasoning.[25] These two worlds are simply the sensible or physical and metaphysical worlds.[26] Plato argues that living organisms, such as, the people, animals and plants inhabit these worlds.[27] Accordingly, intelligible or synthetic things, such as the technologies, necessitate an investigation of their position in the physical and metaphysical worlds. The principle that technology regulations have to examine the "whole" or "wholeness" of the technologies themselves guide this investigation.[28] In other words, the systems[29] or networks[30] that characterise the

23 The Law Society of South Africa (LSSA) "Comments by the Law Society of South Africa (LSSA) on the Cybercrimes and Cybersecurity Bill" https://www.lssa.org.za/wp-content/uploads/2020/01/LSSA-CYBERCRIMES-AND-CYBERSECURITY-BILL-Comment-30-Novemeber-2015.pdf (accessed 2021-03-11).

24 LSSA.

25 Huard *Plato's Political Philosophy: The Cave* (2007) 35-37 and Solomon and Higgins *The Big Questions: A Short Introduction to Philosophy* 8th ed (2010) 121-123. A theory may be defined as 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". See, Morgan and Yeung *An Introduction to Law and Regulation: Text and Materials* (2007) 16.

26 Huard.

27 Huard.

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

29 A system is a contrivance that facilitates the generating, sending, receiving, storing, displaying or processing data messages and includes the Internet. See, s 1 of the ECT Act.

technological wholeness have to be analysed.[31] This paper lucidly makes this analysis. In doing so, the discussion made forms part of four sections. Section 2 studies some of the theories that inform or could inform ICT regulations. Generally, the theories are vast and sometimes diverge. For that reason, only the theories that support the study of regulating disruptive technologies have relevance to this section. The latter relate to those entities that operate independent of human control and intervention. Section 3 examines some of the related laws that are or could be impacted for technology regulations. This includes a discussion of some of the related aspects of the law of property, that is, ownership as a right, and criminal law, that is, attributing responsibility for conduct or acts carried out by machines. The last section is the conclusion. In this section, a summary of the facts examined in the previous sections is made. Thereafter, a conceivable approach to regulate the disruptive technologies is presented.

2 Regulatory theories

2 1 Artificial Immune System (AIS) Theory

The biological operation of the human body is the basis for the Artificial Immune System (AIS) theory. Specifically, the manner in which the biological immune system (BIS) shapes the idea for the AIS Theory.[32] For example, the BIS has a number of cells, molecules or lymphocytes, macrophages, dendritic cells, natural killer cells, mast cells, interleukins and interferons.[33] These cells or molecules allow the physical body to identify infections or viruses from external elements, that is, the so-called "pathogens".[34] Once identified, they then provide a shield or defence mechanism for the organic body.[35] In doing so, the BIS follows a very sophisticated approach in identifying these pathogens. Particularly, it categorises the attacks into self-attacks and non-self-attacks. Self-attacks include the attacks that are known and recognised by the system. Non-

30 A network referred to two or more inter-connected or related computer devices, which allows these inter-connected or related computer devices to exchange data or any other function with each other; exchange data or any other function with another computer network; or connect to an electronic communications network. S 1 of the Cybercrimes Bill.

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

32 Lee, Kim and Hong "Biological Inspired Computer Virus Detection System" in Ijspeert, Murata and Wakamiya (eds) *Biologically Inspired Approaches to Advanced Information Technology* (2004) 153-165 155.

33 Hofmeyr and Forrest "Immunity by Design - An Artificial Immune System" in *Genetic and Evolutionary Computation* (Papers presented at the Genetic and Evolutionary Computation Conference (1999) 1289-1296 1290.

34 Freschi, Coello and Repetto "Multiobjective Optimisation and Artificial Immune Systems: A Review" in Mo *Handbook of Research on Artificial Immune Systems and Natural Computing: Applying Complex Adaptive Technologies* (2009) 1-21 2.

35 Rowe GW *Theoretical models in biology: the origin of life, the immune system and the brain* (1994) 121.

self-attacks arise because of the body or system having been exposed to external danger, for example, bacteria and viruses.[36]

Recognising and categorising self from non-self-attacks is an intricate process. Generally, the system reports and sends alarm signals from injured tissues or cells.[37] These signals are empowered with pattern recognition receptors that study the injuries and evaluate the nature and amount of the required interventions. Following this, the BIS breaks down the attacks into small pieces to restore a suitable balance in the system.[38] If a balance cannot be restored, the system is then immunised to enhance its ability to respond to the attacks. Indeed, the immunisation process is not as straightforward as it seems. For example, there are those who ask what would happen in circumstances where a system attacks itself and subsequently registers the attacks as non-self-attacks?[39] Well, it is possible for self and non-self-attacks to be present at the same time. However, this presence should not destabilise the system and the manner in which it operates. Therefore, the fact that the attacks originate from the system (self-attacks) does not mean that the immunisation process becomes insignificant.

As postulated earlier, the success of the BIS necessitated the development of the AIS theory. This theory came about because of the need to develop flexible and dynamic codes, dispersals and networks that mimic biological cells and molecules.[40] These networks and codes allow programmes and software to be installed, erased and re-installed whenever there is a necessity, new computer users to emerge almost every day and systematic configurations to be flexible depending on imminent self and non-self-attacks.[41]

For technology regulation, the AIS theory promotes the creation of an artificial immune system, that is, the AIS. The AIS detects attacks in a system, for example, a computer, and breaks these attacks down into self and non-self-attacks. Firstly, the breaking down of attacks assists in quantifying damages to the system by, inter alia:

> "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*)."[42]

---

36 Rowe.
37 Matzinger "The Danger Model – A Renewed Sense of Self" 2002 *Science* 301-305 301.
38 Matzinger.
39 Seker, Freitas and Timmis "Towards a Danger Theory Inspired Artificial Immune System for Web Mining" in Scime (ed) *Web Mining: Applications and Techniques* (2005) 151.
40 Birke *Feminism and the biological body* (1999) 142 and Dasgupta, Yu and Nino "Recent advances in artificial immune systems – models and applications 2011 *Applied Soft Computing* 1574-1587 1574-1575.
41 Hofmeyr and Forrest 46.
42 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) 141-148 141.

Secondly, the process of detecting the attacks involves the building of a set intrusion detection algorithms.[43] These algorithms identify, sense and report external anomalies to a system.[44] These could be the illegal use, exploitation and abuse (intrusions) of computer systems. Thereafter, the system will match the anomalies with the identified self or probed intrusions. In cases where a match is found, or the anomaly or anomalies reach an established threshold, the detectors are automatically activated.[45] The activation is then reported to an operator who evaluates and appraises the nature and extent of the anomaly or anomalies.[46] To do this, a risk-sensitive based approach may be necessary to rid the system of identified and sensed anomalies. The latter necessitates that the extent of the attacks determine the apposite responses (immunisation) to breakdown the anomalies to manageable sizes. In each case, the higher the risks posed to the system, the higher the responses adopted to curtail the anomalies is or will be.

One of the examples of technologically empowered BIS is the idea for Intelligent or Smart Grids.[47] This notion arises following the postulated move from an Information Society to a Smart Society. In both these societies, there is a "high level of information intensity in the everyday lives of most citizens".[48] Furthermore, governments, businesses and consumers transmit, receive and exchange data speedily between jurisdictions notwithstanding the distance.[49] However, Smart Societies are a further development of Information Societies.[50] Simply, they are inter-connected societies in terms of which the data, for example, relating to government, agricultural, health energy, transport, etc., on how these societies operate is immediately available and accessible.

Consequently, Smart Grids are one of the technological developments associated with Smart Societies. They are electricity systems and networks (transmission and distribution) that enhance the delivery of sustainable, economic and secure electricity supply.[51] Furthermore, they

43 Aickelin and Cayzer 148.
44 Aickelin and Cayzer 148.
45 Aickelin and Cayzer 148-149.
46 Aickelin and Cayzer 150.
47 The other example is the system referred to as the Intelligent Water Management or Smart Water Grid. See, Tsakalides et al *Smart Water Grids: A cyber-Physical Systems Approach* (2018), Owen (ed) *Smart Water Technologies and Techniques: Data Capture and Analysis for Sustainable Water Management* (2018) and Roy and Bhaumik "Intelligent Water Management: A Triangular Type-2 Intuitionistic Fuzzy Matrix Games Approach" 2018 *Water Resour Manage* 949-968.
48 Durrani S *Information and Liberation: Writings on the Politics of Information and Librarianship* (2008) 256 and Manning T *Radical Strategy: How South African Companies Can Win Against Global Competition* (1997) 134.
49 Durani.
50 Dameri RP "Urban Tabeau de Bord: Measuring Smart City Performance" in Mola L, Pennarola F and Za S (eds) *From Information to Smart Society: Environment, Politics and Economics* (2015) 173-180 at 173-179.
51 Smart Grids seek to, inter alia, provide proficiency in the transmission of electricity, facilitate speedier restoration of electricity after power

augment the reliability, availability and efficiency of the existing energy control mechanisms. Ordinarily, IoT sensors, wireless sensor node (WSN),[52] digital meters and controllers are attached to the grid.[53] The rationale for this is to assist in identifying and reporting power outages electronically.[54] Using the BIS method, the IoT sensors package the identified or imminent power interruptions. Thereafter, they send or transmit power-specific signals to a remote operator.[55]

2 2 Theory for *Lex Informatica*

Law Merchant (*Lex Mercatoria*) is the foundation for the principle for *Lex Informatica*. The latter is the branch of the law that developed in the Middle Ages and propelled by the practices associated with the Feudal System.[56] This law was inter-national in its nature, in that, it regulated the affairs of the various nation (feudal) states.[57] Furthermore, it embodied the practices and customs followed by the diverse secular states.[58] Given inter-national nature, Law Merchant was so flexible that it could respond to the applicable domestic practices adopted by different states.[59] For example, it existed following the inadequacy of national laws to regulate cross-border trading. Accordingly, Law Merchant provided solutions to determine and settle the related trans-national merchant disputes. Furthermore, it became necessary to expand its reach in a manner that allowed this law to deal with the prevailing business and market improvements.[60] In other words, business and market growths required a development of merchant rules and principles.[61]

---

disturbances, reduce operations and management costs for utilities, and ultimately lower power costs for consumers, decrease peak demand, which will also help lower electricity rates, augment integration of large-scale renewable energy systems, cascade the integration of customer-to-owner power generation systems, including renewable energy systems, and improve the energy security. See, Owen 2-3.

52 WSNs are nodes that collects, processes and dissemination information or data through virtual networks. They consist of various online sensing devices and these devices facilitates identifying, segregating monitoring and measuring the quality and quantity of information stored online. See, Vujovic and Maksimovic "Raspberry Pi as a Wireless Sensor Node: Performances and Constraints" 2014 *MIPRO* 1247-1252 1247.

53 Tsakalides et al 4-7.

54 Tsakalides et al 4-7.

55 Owen 2-3.

56 Johnson and Post "Law and Borders – The Rise of Law in Cyberspace" 1996 *Stanford Law Review* 1366-1402 1389.

57 Pollock and Maitland *The History of English Law Before the Time of Edward I* 2nd (1968) 467 and Trakman "From the medieval Law Merchant to E-Merchant Law" 2003 *University of Toronto Law Journal* 265-304 265.

58 Trakman 265.

59 Academy of International Law *Recueil Des Cours 273 (1998)* (1999) 393.

60 Mefford "*Lex Informatica* – Foundations of Law on the Internet" 1997 (5) *Indiana Journal of Global Legal Studies* 211-237 223-224.

61 Mefford.

Following the dynamic nature of the Law Merchant, Reidenberg developed what he referred to as the *Lex Informatica*.[62] His hope for *Lex Informatica* was that the latter would be able to progress with the developments in technologies. This denotes a situation where a connection exists between technological regulations and the technology that informs the regulations. Consequently, Reidenberg used as the point of departure the fact that legal regulations are the elementary structure of the law or *lex*.[63] In other words, they become instruments or tools to channel the behaviour of society.[64] To facilitate this process, the command and control principle is usually applied. However, *Lex Informatica* depends on the architectural standard of the Internet, for example, the HTTP and the defaults as the basic structure for ICT regulations.[65] Furthermore, it relies on certain default rules, the formulation of which is separate from the law-making process. Commonly, the developers or engineers of the technologies build and generate these rules. The rules cover, inter alia, the position of technologies in society, that is, their social construction or process.[66] In this manner, the technological architecture imposes regulations on the users of technologies.[67]

Lessig similarly supports the view of technology-imposed regulations. He argues that technologies regulate in terms of certain codes or computer-generated codes (keys), for example, PINs, Usernames and Passwords.[68] This is the position because technologies necessitate the migration from offline to online spaces (cyberspace). This arises because, according to Lessig, cyberspace is a space where:

> "People meet, and talk, and live….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 (regulators) should know something about their form, and more about their potential".[69]

In the main, the choices in the design of technologies determine the nature of the computer codes available to the cyberspace.[70] For example, the design of the technologies also assist in controlling the accessing or not of the technologies. This access depends on whether a person possesses the correct code to unlock access.[71] Therefore, *Lex Informatica* concedes that the starting point to ICT regulations is the

62 Reidenberg "*Lex Informatica* – The Formulation of Information Policy Rules Through Technology" 1998 *Texas Law Review* 553-584.
63 Reidenberg.
64 Hood and Margetts *The tools of government in the digital age* (2007) 2.
65 Reidenberg.
66 Reidenberg.
67 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.
68 Lessig *Code and Other Laws of Cyberspace* (1999) and Lessig "The Path of Cyberlaw" 1995 *The Yale Law Journal* 17-46.
69 Lessig.
70 Ong *Mobile Communication and The Protection of Children* (2010).
71 Paré 54.

proper understanding of the technologies themselves. This is because the technological architecture, for example, the codes, usernames or passwords, imposes regulations on who should access these technologies.

Having discussed the selected ICT regulatory theories, it is evident that they discard an ICT regulatory structure modelled on legal rules. As such, they accept that understanding technologies should inform ICT regulations. In this manner, the theories may fairly do well in regulating technologies arising consequent to the Third Industrial Revolution, for example, the Internet and the World-Wide-Web. However, they do not adequately cover the developments arising following the 4IR (disruptive) technologies. Specifically, they fail to appreciate that some of the disruptive technologies, for example, AI, have cognitive abilities and that they can operate independent of human control and interventions. Instead, the theories assume that technology regulations control the behaviour of users online. In other words, users migrate online based on them possessing an authentication code, username or password. Thus, the system grants access to users who possess the correct authentication code and deny access to those who do not. Therefore, this presupposes a situation wherein users have control over the code, username or password as a specific regulatory tool. In addition, the theories do not envisage that 4IR technologies are able to generate other technologies or of re-generating themselves in ways that do not require human control and guidance.[72] Conversely, they postulate that the technological codes over which users have control are suitable regulations for the control of ICTs.

In view of the above-mentioned, the sections below examine the element of "(human) control" when dealing with disruptive technologies. This study scrutinises some of the relevant principles of the law relating to ownership and control. This has to do with studying the applicable provisions of the law of property. Thereafter, a discussion is made of the related principles of criminal law, that is, the attribution of criminal responsibility. The rationale for this is to determine whether artificial intelligence (AI) can control other machines or robots.[73] Furthermore, it is to establish whether there is or could be such a thing as a "reasonable AI, machine or robot" for factual and legal purposes.

72 Tegmark *Life 3.0: Being Human in the Age of Artificial Intelligence* (2017) 23.

73 AI are synthetic or man-made machines or robots that are equipped with the cognitive capability similar to that of humans. They include autonomous robots that can respond to a wide range of consternations and follows a particular problem-solving technique. See, Mainzer *Artificial Intelligence – When Do Machines Take Over?* (2020) 2.

3 Selected legal principles

3 1 Background

The ICT regulatory theories assume that ownership and control are the prerequisite for ICT regulations. Thus, a control of an authentication code, username or password determines this control. Should the correct code, username or password be absent or could not be located, required access to an online system could consequently be denied. In terms of the AIS theory, this absence triggers an anomaly-detection process. The effect of this is for the system to reject the requested access on the basis that the granting is or will likely expose the system to external (non-self) attacks. For *Lex Informatica*, the absence of the required code results in a user remaining in offline spaces. This follows the system henceforth declining a user the requested migration to cyberspace.

Therefore, the theories do not deal with situations where human control is not a factor for the effective and efficient operation of disruptive technologies. Given this, it has become indispensable to investigate questions regarding who or what controls these 4IR technologies. This study looks at the nature and essence of the ownership as a right. The idea is not to seek to re-write property law as such. Simply, it is to understand whether the notion of "control" in the law of ownership is elastic or capable of developing. Following this, a determination is made on whether control is central to the attribution of legal responsibility for acts a machine or robot carry out independently of human control. The related aspects of criminal law, that is, criminal responsibility, assist in making or determining this attribution.

3 2 Ownership and control

Generally, the essence of control, in terms of the law of property, is a flexible one. It is adaptable to changes that occur to society. This flexibility does not affect, however, the principle that the basis of control is the acceptance of a relationship that exists between a person and thing.[74] Old Roman law recognised this relationship in the Laws of Twelve Tables.[75] For example, Table IV.V of the Twelve Tables states that only Roman citizens could assume control of or over things. This assumption did not translate to ownership as such. It had relations to the fact, inter alia, that:

> "The technical word for ownership of things: it (ownership) was an element of the house-father's *manus*. In time, although it is impossible to say when, the word *dominium* came into use; but, so far as can be discovered, it did not occur in the Tables, and must have been of later introduction. In those days,

74 Njotini "Examining the 'Objects of Property Rights' – Lessons from the Roman, Germanic and Dutch Legal History" 2017 *De Jure* 136-155 154-155.
75 Hereinafter referred to as the Twelve Tables.

> when a man asserted ownership of a thing, he was content to say, - 'It is mine,' or 'It is mine according to the law of Quirites."[76]

Pre-classical and classical Roman law also followed this old Roman law formulation of control. However, classical Roman law introduced, for first time, the notion of ownership or *dominium* to the Roman law study of property law.[77] In this manner, the element of control of or over property is inferred from this classical Roman law concept of *dominium*. Well, the notion was altered a number of times, for example, in post-classical, Germanic law, Medieval law, Sixteenth century (*mos italicus, mos gallicus,* moral philosophers), the Pandectists (private law dogma) and Dutch law. However, the classical Roman law formulation of control remains the finest in the history of the law of property. Specially, it is during this period that ownership was defined very broadly to include certain other rights, for example, the right to use, enjoy, destroy and transfer a thing.[78]

Now that ownership has to do with control of or over things, the next stage of the inquiry is what were the things over which control was exercised? Classical Roman law described those things as the objects that are of economic value to a person.[79] These were the *res in commercio*.[80] Consequently, control was possible or only conceivable in respect of those objects or things that guaranteed economic interest of a monetary value.[81] These were both corporeal property (land, house, horse, slave, garment, gold or silver) and incorporeal property (rights,[82] inheritance, servitude or *hereditas*).[83]

It is possible that South Africa follows the classical formulation of ownership and control. Particularly, South Africa accepts that the notion of *dominium* is symbolical to the "control" a person has over property. Some academics regard this control as connoting the power that a person has over a thing, that is, the *ius in rem suam*.[84] However, South Africa extends the objects of property or rights in property beyond *res in*

---

76 Muirhead *Historical Introduction to the Private Law of Rome* (1998) 126. See also, Bouckaert "What is Property?" 1990 *Harvard Journal of Law and Public Policy* 775-816 781.

77 Schulz *Classical Roman law* (1961) 338-339.

78 Garnsey *Thinking About Property: From Antiquity to the Age of Revolution* (2007) 177, Buckland *A Manual of Roman Private Law* (1939) 111 and Buckland *The Main Institutions of Roman Private Law* (1931) 93.

79 Garnsey.

80 Kaser *Roman Private Law* (translated by Dannenbring R) (1980) 80.

81 Moussourakis *Fundamentals of Roman Private Law* (2012) 119.

82 A right in property is a legally justified entitlement or interest. See, Van der Walt and Pienaar *Introduction to the Law of Property* 6th ed (2009) 13. It gives a person (legal person) a valid claim to or over property (a legal object) as against other persons. See, Badenhorst, Pienaar and Mostert *Silberberg and Schoeman's the Law of Property* 5th ed (2006) 9.

83 Sohm *The Institutes: A Textbook of the History and the System of Roman Private law* 3rd ed (1907) 225.

84 Van der Walt and Kleyn "Duplex Dominium – The Theory and Significance of the Concept of Divided Ownership" in Visser (ed) *Essays on the History of*

commercio. In other words, it also included those things that are of sentimental value to a person, for example, a photograph. These could be both corporeal and incorporeal things. On the one hand, corporeal things are, among others, a horse, furniture, vehicle, motorbike, cylinder with oxygen, landed property or fruits that still hang on the tree.[85] On the other hand, incorporeal things include a right, duty, credit[86] or share,[87] electricity,[88] servitude or inheritance.

Important to the study of property as an object of rights in South Africa is the distinction between private and public rights. Firstly, private rights have basis on private law, that is, the law regulating the relationship between individuals in society, for example, the law of property.[89] Because of this relationship, a person acquires a legally recognised claim over a thing.[90] Secondly, Chapter 2 of the Constitution of the Republic of South Africa, 1996[91] enshrines the public rights. Specifically, section 25 of the Constitution (the "Property Clause") enumerates the public rights to property in South Africa. Therefore, studying these developments is essential in properly understanding the evolution of property as a right in South Africa. For example, it assist in appreciating the relevance of the so-called "dephysicalisation of property" to the study of control of or over things.[92] The latter notion exists because of the acceptance that:

> "Complex social, economic and legal processes by which incorporeal or intangible property are becoming increasingly important for personal wealth and security and for social welfare, while the importance of traditional tangible property such as land declines."[93]

The dephysicalisation of property accepts that control for purposes of the law of property does not only apply to the traditional forms of things. However, it can also arise in respect of another or other subjective rights, for example, real rights,[94] personality rights,[95] intellectual property

Law (1989) 213 213 and Hosten and Schoeman "Private Law – Law of Things" in Hosten et al (eds) *Introduction to South African Law and Legal Theory* (1997) 622-659 624.

85 Van der Walt and Pienaar 14.

86 See, *S v Kotze* 1961 (1) SA 118 (SCA).

87 *Cooper v Boyes No and Another* 1994 (4) SA 521 (CPD) 535B-C.

88 *Froman v Herbmore Timber and Hardware (Pty) Ltd* 1984 (3) SA 609 (W) 610I. For further interesting reading, see, *Naidoo v Moodley* 1982 (4) SA 82 (TPD).

89 Neethling and Potgieter *Neethling-Potgieter-Visser Law of Delict* 7th ed (2015) 3.

90 Badenhorst, Pienaar and Mostert 9.

91 Hereinafter referred to as the Constitution.

92 Vandevelde "The New Property of the Nineteenth Century – The Development of the Modern Concept of Property" 1980 *Buffalo Law Review* 325-367 333.

93 Van der Walt *Constitutional Property Law* (2005) 66.

94 Where the object of right is a thing, it is presumed that real rights accrue to the property. See, *Cape Explosive Works Ltd and Another v Denel (Pty) and others* 2001 (3) SA 569 (SCA) 20.

rights[96] or personal rights.[97] Accordingly, property rights over other property rights are possible in South Africa.[98]

Having examined the above-mentioned, it is evident that the notion of control has basis on a flexible and adaptable system of the law. Specifically, the developmental state of society determines the meaning to be attributed to control. In other words, it signifies the nature and extent of control to be exercised in each case. In turn, studying control requires an investigation to be made of the societal developments. This view is particularly true of South Africa. For example, South Africa accepts that circumstances may exist that necessitate the dephysicalisation of control. Following this, the requisite control may not necessarily be in relation to corporeal or incorporeal objects. However, it may be over other rights in respect of corporeal and incorporeal things.

Therefore, the question is what is the relevance of this dephysicalisation of control to the necessity to regulate disruptive technologies? The sections below provide a suitable attempt to respond to this question.

3 3 Legal (criminal or civil) responsibility

Generally, attributing criminal or civil responsibility is the product of history. In the law of delict, for example, it has basis to the fundamental principle of the *res perit domino*.[99] This principle rests on the premise of the law that "damage or harm rests where it falls".[100] In other words, a person bears the damage or harm he or she suffers.[101] Thus, a person, A, has no legal ground for complaint in situations where lightning struck him on his way home. For delictual purposes, this implies that, for damage or harm to rest where it fall, a person, that is, a wrongdoer, must have caused the damage to A.[102] Now, the question is what would happen in circumstances wherein the wrongdoer is not a person, but is a machine or robot? Let us explain this situation by means of an example: In 1981, a robot killed a 37-year-old Japanese employee of a motorcycle

95 These are the rights that a person has to his or her physical or psychological wellbeing. They are claimed or claimable in delict where damage or harm was caused to a person.

96 Intellectual property rights include those rights that are a creation of a person's mind, for example an invention or symbol. See, Van der Walt and Pienaar 307-312.

97 These rights are, inter alia, a claim for specific performance. See, Hosten et al *Introduction to South African Law and Legal Theory* 2nd ed (1997) 625.

98 Hosten et al.

99 Neethling and Potgieter 3.

100 Neethling and Potgieter.

101 *Imvula Quality Protection (Pty) Ltd v Loureiro* 2013 (3) SA 407 (SCA) 418 and *Telematrix (Pty) Ltd t/a Matrix Vehicle Tracking v Advertising Standards Authority SA* 2006 (1) SA 461 (SCA) 468.

102 Indeed, causation is one of the elements a person (plaintiff) should allege and prove for another person (defendant) to be held liable in delict. The other elements are an act, wrongfulness, fault and harm. See, Neethling and Potgieter 4.

factory. The robot made an error of judgement by identifying the employee as a risk to its intended (programmed) mission. It then calculated that the most effective way to remove this ostensible threat was to push or squeeze it into an adjacent operating machine. Using its very commanding hydraulic arm, the robot shattered the shocked worker into the operating machine, killing him instantly. Following this, the machine resumed with its duties as if nothing had happened. Consequently, the question was who or what could be held responsible for the killing of the employee?

Well, a strict application of the *res perit domino* principle will conclude that damage or harm does not rest on the machine. In other words, the machine is not a person for purposes of determining wrongfulness in delict. Furthermore, one would be inclined to invoke the notion of control to establish who had control over the machine. In this endeavour, an attempt would be made to ascertain whether the requisite control was exercised or carried out in line with or for the purpose for which the machine was programmed. Simply, finding a suitable answer to the above-mentioned questions is fundamentally a cumbersome process. However, the starting point in attempting to get a reasonable response should be to distinguish between:

- Instances wherein where technologies follow the instructions of a human or carries out an act under the direction and control of a human.
- Instances wherein technologies act without the required direction and control, that is, independent of human direction and control.

In relation to the first-mentioned occurrence, the ordinary principles of criminal law would apply. Simply, the technology is merely an instrument, similar to a knife or gun, which a human would use in carrying out the act. Accordingly, the fact that technologies carry out the act is indecisive. It is sufficient if the requisite act or *actus reus* and mental state (*mens rea*) of a human in the form of an intention to carry out the act is present. Because of this, the actions of the technologies are or would be attributed to those of a human.

As regards the second-mentioned circumstances, the positions seems to be more burdensome. This is the position because disruptive technologies possess the cognitive abilities that render an inquiry into the required control insignificant. Specifically, these technologies operate autonomously and can produce and re-produce themselves and other disruptive technologies.[103] As a result, the determination is not so much about who or what controls these technologies. Rather, it includes an investigation of the place where legal responsibility vests in situations where technologies operate independently and autonomously. There are many reasons why an inquiry of this nature is essential. Firstly, it assists in responding to the question regarding whether human control prevails or is the only *sine qua non* for the operation of AI. Secondly, it helps in

103 Turner *Robot Rules: Regulating Artificial Intelligence* (2019) 4.

determining whether the disruptive technologies have become so autonomous that human control has now become inconsequential. Simply, has society reached a stage wherein disruptive technologies ought to be studied as independent entities with their distinctive rights and obligations?

Hallevy authored a book titled *When Robots Kill: Artificial Intelligence under Criminal Law*. In this book, he identified some of the challenges emanating from technologies operating independently of human control by stating the following:

> "Robots and computers are more frequently replacing humans in performing simple activities. As long as humanity used computers more as tools, there was no significant difference between computers and screwdrivers, cars, or telephones. But as computers became increasingly sophisticated, we started saying that they 'think' for us. The problem began when computers evolved from 'thinking machines' (devices programmed to perform specific thought processes, such as computing) into thinking machines without the quotation marks – in other words, artificial intelligence."[104]

Consequent to this identification, Danaher posits that there is generally a "mismatch between the human desire for retribution and the absence of subjects of retribution blame".[105] He refers to this mismatch as the "retribution gap". Retribution gap exists when a determination has to be made about how to allocate (civil and criminal) responsibility between humans and robots or between machines or robots themselves.[106] In fields such as the law of delict, the mismatch is elongated in certain circumstances. This is particularly the case because, sometimes, some acts or conduct are expected of a reasonable person or should be judged using the standard of a reasonable person or the *boni mores* criterion and others are not.[107] For example, in the case of *Lee v Minister for Correctional Services*,[108] the court stated that:

> "Our law has reached the stage of development where an omission is regarded as unlawful conduct when the circumstances of the case are of such a nature that the legal convictions of the community demand that the omission should be considered wrongful. This open-ended general criterion has since evolved into the general criterion for establishing wrongfulness in all cases, not only omission cases."

104 Hallevy *When Robots Kill: Artificial Intelligence under Criminal Law* (2013) xv.

105 Danaher "Robots, Law and the Retribution Gap" 2016 *Ethics and Information Technology* 299.

106 Danaher.

107 *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T) 387. See also, *Steenkamp NO v Provincial Tender Board, Eastern Cape* 2007 (3) SA 121 (CC) 139, *Phumelela Gaming and Leisure Ltd v Grndlingh* 2007 (6) SA 350 (CC) 361–362, *Marais v Richard* 1981 (3) SA 1157 (A) 1168 and *Minister van Polisie v Ewels* 1975 (3) SA 590 (A) 597.

108 *Lee v Minister for Correctional Services* 2013 (2) SA 144 (CC) 167.

According to *International Shipping Co (Pty) Ltd v Bentley*, the wrongful or unlawful act is "linked sufficiently closely or directly to the loss".[109] It really does not matter whether the loss is too remote.[110]

Given the above-mentioned, an inquiry is made regarding whether it is possible to expect a machine or robot to act reasonably. Alternatively, is it fair and reasonable to attribute the standard of a reasonable person to a machine or robot? In seeking to respond to these questions, Hallevy introduces the three models[111] or the "Matrix of Derivative Criminal Liability".[112] He calls these the "Perpetration-via-Another Liability Model", "Natural-Probable-Consequence Liability Model" and 'Direct Liability Model".[113] The first model regards a machine as an innocent agent that do not possess any human attributes, for example, memory, cognition and independent operation.[114] Specifically, it excludes the possibility of machines carrying out certain acts resulting in the attribution of responsibility. According to Hallevy, the disruptive technology, inter alia:

> "… resembles the parallel capabilities of a mentally limited person, such as a child, or a person who is mentally incompetent and thus lacks a criminal state of mind".[115]

Thus, the least that could happen is that "perpetrator-via-another" could ensue. In this instance, the principal becomes the perpetrator by means of his or her conduct and *mens rea*.[116]

The second model looks at the involvement of the programmers and users of the technologies.[117] Particularly, it requires that an examination of a specific program, for example, human pilot, be made to determine the allocation of responsibility.[118] Pagallo argues that this model presents two possibilities. Firstly, it relates to:

> "The hypothesis of *Picciotto Roboto* by design, insofar as it is defined as programmers, manufacturers or users who intend to commit a crime through

109 *International Shipping Co (Pty) Ltd v Bentley* [1990] 1 All SA 498 (A) 700.
110 *International Shipping Co (Pty) Ltd v Bentley supra,* 700.
111 Hallevy "The Criminal Responsibility of Artificial Intelligence Entities – From Science Fiction to Legal Social Control" 2016 *Akron Law Journal* 171-219 174. See also, Hallevy *Liability for Crimes Involving Artificial Intelligence Systems* (2015) 82-112.
112 Hallevy *The Matrix of Derivative Criminal Liability* (2012) 63-138.
113 Hallevy 138.
114 Hallevy 179.
115 Hallevy "Criminality Liability for Intellectual Property Offences of Artificial Intelligent Entities in Virtual and Augment Reality Environments" in Barfield & Blitz (eds) *Research Handbook on the Law of Virtual and Augmented Reality* (2018) 389-420 400. For furthermore interesting reading see, Hallevy *When Robots Kill: Artificial Intelligence Under Criminal Law* (2013).
116 Hallevy.
117 Hallevy 181.
118 Pagallo *The Law of Robots: Crimes, Contracts, and Torts* (2013) 71.

Picciotto Roboto, but the latter deviates from the plan and commits some other offence".[119]

Secondly, it excludes the intent to commit a wrong and evinces negligence on the part of the programmers or manufactures or users when designing, constructing or using the machine.[120] Consequently, the inquiry relates to whether the programmers, manufactures or users had foreseen or could reasonably have foreseen the possibility of the technologies carrying out an act or conduct.[121] Conversely, the investigation is whether the harm or damage is or was the natural or probable consequence of the wrong carried out by the machine or robot.[122]

The third model examines the technologies as an independent entity. Accordingly, it requires consideration to be made of both the internal (the algorithms) and external elements (software and hardware) of the technologies.[123] Here, the question is whether the entity failed to exercise due and reasonable care in the circumstances.[124] In this instance, the behaviour or activities of the agent, that is, the programmer, manufacturer or user of the robot, are indecisive.[125] It is sufficient if the entity failed or omitted to take due and reasonable measures of care to prevent a wrong from occurring.[126]

As convincing as the models Hallevy champions are, they, however, do not adequately address some of the questions raised in this paper. Specifically, these models are still attached to the notion of control. In other words, they follow the idea of always determining "who controls and owns the disruptive technologies". In addition, they do not explore the possibility of machines acting reasonable or unreasonable for legal purposes. To this end, the Matrix of Derivative Criminal Liability may have reasonably addressed some of the technological developments at the time (in 2010) when Hallevy first published his paper. However, they do not adequately address the current regulatory challenges that these disruptive technologies continue to generate. Furthermore, the fact that Hallevy refers to Asimov's Three Laws of Robotics does not justify this insufficiency.[127]

119 Pagallo.
120 Pagallo.
121 Hallevy 101 182.
122 Hallevy.
123 Hallevy.
124 Lehner "The Australian Model of Attributing Criminal Responsibility to Legal Entities" in Brodowski, De la Parra, Tiedemann and Vogel (eds) *Regulating Corporate Criminal Liability* (2014) 79-86 81.
125 Lehner.
126 Lehner.
127 These are that a robot may not injure a human being or, through inaction, allow a human being to come to harm (Law 1), a robot must obey the orders given to it by human beings except where such orders would conflict with Law 1 (Law 2) and a robot must protect its own existence as long as such protection does not conflict with the Laws 1 and 2 (Law 3). See, Asimov *The Three Laws* (1981) 18.

4 Conclusion

Disruptive technologies that the 4IR generates have radical or disruptive effects on an information society. The impact extends beyond the provision of paradigm shifts or transformations on the economy, business and consumers. It furthermore relates to these technologies blurring the lines between that which is physical, digital and biological domains. Flowing from these developments are uncertainties regarding the manner and structure of technology regulations. Generally, there are numerous reasons why these regulatory uncertainties exist. Firstly, there is a need for society to embrace disruptive technologies. This need fosters the taking advantage of developments in technologies. Secondly, society must stablish measures to control and ameliorate the associated technological setbacks, for example, the re-structuring of businesses or economy. Now, this necessity compels a complete understanding of the position of disruptive technologies on society. For example, Richard Susskind argues that legal regulations play a dominant function for technological control.[128] However, there is a danger, Susskind continues, of legal regulations lagging behind or continuously playing catch-up with developments in technologies. To avert this, regulators are likely to introduce inchoate legal regulations. The latter includes regulations that encourage the re-invention of the technology-regulatory wheel. [129]

Therefore, the question is how should the structure of technology regulations be if disruptive technologies present both the opportunities and setbacks to the information society? Certain regulatory theories are discussed that suggest a postulated overview of technology regulations. The first theory abstract technology regulatory structures from the BIS. The second theory champions the idea of codes for technology regulations. In other words, it surmises that codes are the laws (or *lex*) that regulate the online activities or behaviour. In view of this, there is no necessity to commence or introduce legal regulations outside of the codes. Well, the view of codes as technology regulations is convincing. However, it rests on the premise that the regulatory instrument, that is, the code, is subject to the control of a user or consumer. In other words, the performing of an online activity depends on a person possessing the correct code. The challenge then is that codes do not regulate innovations associated with the disruptive technologies. For example, disruptive technologies do not rely on human control for them to perform a function. Specifically, they can produce other technologies or re-produce themselves without human control or intervention. Consequently, a strict application of codes for technology regulation is problematic.

In this paper, a further extension or development of Hallevy's "Matrix of Derivative Criminal Liability" is proposed. This development should encourage a study of 4IR and 4IR technologies as independent entities.

128 Susskind *The Future of Law: Facing the Challenges of Information Technology* (1996) 2-43.
129 Susskind.

This means discouraging the idea of, for example, measuring the intelligence of an AI or Machine using the intelligence of human. For technology regulations, it is possible to impose penalties (punitive or compensatory) on machines or AI. These penalties could be modelled from those currently existing or are imposed to regulate offline conduct. The examples are, inter alia, the actions for damages and those relating to the sentencing of the accused person. For example, consumers download online applications (Apps) with the object that the App will facilitate their online activities. Should the App fail to achieve such an objective, consumers would impose a death penalty on the App. In other words, they delete the App from their machines or computers and even discourage others from using the App in the future. Another example relates to the determination of reasonableness in the law of delict. For example, it is inquired whether machines or AI can act wrongfully to such an extent that it may be said that they failed to conform to the standard of a reasonable person? There is no reason why machines or AI cannot act in the aforesaid manner. However, it is still necessary for technology regulators to study the dynamics of the disruptive technologies, and examine instances wherein these technologies will benefit society and those where they exacerbate societal setbacks or disparities.