Law Schools Global League

**- Working Group on New Technologies and Law –**

Chicago, 2016

The Group on New Technologies and Law has been working for the past year on gathering, discussing and editing papers that challenge the relationship between law and technology. In order to enable discussions for the 2016 Chicago Academic Conference, we have chosen to assemble short versions of the research that is currently under way – otherwise this document would be far too long for our audience to be able to engage. The editors (Professors Mônica Guise Rosina, Steve Cornellius and Ugo Pagallo) are working on the editing process so that all papares can be jointly published by the end of 2016 @ a special edition of an academic journal.

* If you wish to have access to the full versions of one or more papers, please direct your request to: monica.rosina@fgv.br

## I. Law as Meta-Technology

*By Ugo Pagallo (Turin University), Colette Cuijpers (Tilburg University) and Mônica Steffen Guise Rosina (FGV Law School in São Paulo)*

The starting point of our analysis on law and technology has to do with a basic fact: whereas, over the past centuries, human societies have used information and communication technology ("ICT"), but have been mainly dependent on technologies that revolve around energy and basic resources, today's societies are increasingly dependent on ICT and moreover, on information as a vital resource. The processing of well formed and meaningful data is not only reshaping essential functions of current societies, such as

governmental services, transportation and communication systems, business processes, or energy production and distribution networks. What is more, the information revolution is affecting our understanding about the world and about ourselves. By insisting on the legal impact of the information revolution, it does not follow, however, that the law cannot regulate the process of technological innovation. On the contrary, the law can conveniently be understood as a technique that regulates other techniques and hence, as a meta-technology which competes with other modalities of regulation, such as the forces of the market or of social norms. In addition, the traditional hard tools of the law, such as statutes and codes supported by the threat of physical sanctions, have increasingly been complemented with more sophisticated forms of enforcement via the mechanisms of design, codes, and architecture.

This is the bread and butter of work on the regulatory aspects of technology in such fields as universal usability, informed consent, crime control, social justice, or design-based instruments for implementing social policies. From the viewpoint of the law as a meta-technology that competes with other forms of regulation, we thus assume a bidirectional tension, or interplay, between law and technology. Instead of a one-way movement of social evolution from technology to law, a key component of the legal challenges in an information society concerns the other way around, that is, how the regulatory tools of technology can be exploited by embedding normative constraints into the design of spaces (environmental design), or of objects (product design), or of messages (communication design), so as to comply with the rules of current legal frameworks. On this basis, three different levels of analysis follow as a result, namely (i) the legal impact of technology; (ii) the law conceived as a meta-technology; and, (iii) the field of techno-regulation, or legal regulation by design. More particularly:

(i) The legal impact of technology suggests that focus should be on how the current information revolution is affecting the tenets of the law. In addition to transforming the approach of experts to legal information, e.g. the development of fields such as AI and the law, technology has brought on new types of lawsuits, or modified existing ones. Consider

new offences such as computer crimes (e.g. identity theft) that would be unconceivable once deprived of the technology upon which they depend. In accordance with the clause of criminal immunity summed up, in continental Europe, with the formula of the principle of legality, i.e. "no crime, nor punishment without a criminal law" (*nullum crimen nulla poena sine lege*), this is why international lawmakers decided to intervene with the Budapest Convention on cybercrime in November 2001. Moreover, reflect on traditional rights such as copyright and privacy, both turned into a matter of access to, and control and protection over, information in digital environments. By examining the legal challenges of technology, we thus have to specify those concepts and principles of legal reasoning that are at stake. Then can we begin to determine whether the information revolution: (a) affects such concepts and principles; (b) creates new principles and concepts; or, (c) does not concern them at all, the latter being the view of traditional legal scholars.

(ii) The law conceived as a meta-technology has to do with the old, Kelsenian account of the law as a social technique of a coercive order enforced through the menace of physical sanctions: "if A, then B." To be sure, law can be considered as a form of meta-technology without buying any of Kelsen's ontological commitments. Rather, we should pay attention to the impact of technology on the formalisms of the law, much as how legal systems deal with the process of technological innovation, through such a complex network of concepts, as agency, accountability, liability, burdens of proofs, clauses of immunity, or unjust damages. In this latter case, the aim of the law to govern the field of technological innovation comprises several different approaches. Some, as Bert-Jaap Koops (2006), distinguish four main legislative purposes, such as: (a) the achievement of particular effects; (b) functional equivalence between online and offline activities; (c) non-discrimination between technologies with equivalent effects; and, (d) future-proofing of the law that should neither hinder the advance of technology, nor require over-frequent revision to tackle

such a progress. Others, as Chris Reed (2012), propose to differentiate between (a) technological indifference, i.e. legal regulations which apply in identical ways, whatever the technology, such as the right to authorize communication of a work to the public in the field of copyright law; (b) implementation neutrality, according to which regulations are by definition specific to that technology and yet, they do not favour one or more of its possible implementations, e.g. the signature of e-documents; and, (c) potential neutrality of the law that sets up a particular attribute of a technology, although lawmakers can draft the legal requirement in such a way that even non-compliant implementations can be modified to become compliant.

(iii) The field of techno-regulation, or legal regulation by design, concerns how current advancements of technology have obliged legislators and policy makers to forge more sophisticated ways to think about legal enforcement. Although some of these architectural measures are not necessarily digital, e.g. the installation of speed bumps in roads as a means to reduce the velocity of cars, the new scenarios of the information revolution have suggested national and international lawmakers complementing the traditional hard tools of the law through the mechanisms of design, codes, and IT architectures. Many impasses of today's legal and political systems can indeed be tackled, by embedding normative constraints and constitutional safeguards into ICTs. Whereas, in their work on *The Design with Intent Method* (2010), Lockton, Harrison and Stanton describe 101 ways in which products can influence the behaviour of their users, suffice it to dwell here on three different aims that design may have: (a) to encourage the change of social behaviour through incentives based on trust (e.g. reputation mechanisms), trade (e.g. services in return), etc.; (b) to decrease the impact of harm-generating behaviour through security measures, user-friendly interfaces, default settings, and the like; and, (c) to prevent harm-generating behaviour from occurring via the use of self-enforcing technologies. The latter appears the most critical aim

of design, since people's behaviour would unilaterally be determined on the basis of technology, rather than by choices of the relevant political institutions and moreover, the normative side of the law would be transferred from the traditional "ought to" of legal systems to what actually is determined by technical instructions. Leaving aside China's "Great Firewall" and the systems of filters and re-routers, detours and dead-ends, which aim to keep internet users on the state-approved online path, it is noteworthy that the repressive side of this design policy has shown up in Western democracies as well (Pagallo 2015). Two challenges to the rule of law are particularly striking. On the one hand, the use of allegedly perfect self-enforcing technologies raises serious threats of paternalism and, even, of authoritarianism, because such techniques as DRMs, automatic versions of the principle of privacy by design, three-strikes approaches to copyright enforcement, or systems of filters in order to control the flow of information on the internet, end up with the modelling of individual conduct. On the other hand, the aim of both lawmakers and private companies to increasingly tackle the challenges of the information era through the means of design, code, and IT architectures, that is, by embedding legal safeguards into information technology, often leads to the illegitimate condition where states claim to regulate unilaterally extraterritorial conduct by imposing norms on individuals who have no say in the decisions affecting them.

In accordance with this tripartite differentiation on law and technology, the intent of the paper is to further our understanding of the interplay between the legal impact of today's information revolution and the regulatory aims of the law, in light of some relevant practical cases for analysis, such as Uber and sharing economy business models, e-voting, virtual goods, ISP liability, copyright and data protection, encrypted currencies, security and online trust. These cases suggest that we should draw attention to whether, or to what extent, technology is impacting basic tenets, principles, or concepts of the law and, vice versa, how the law intends to govern such fields. Should we endorse the criterion of

functional equivalence between off-line and ICT-driven activities, or rather the principle of implementation neutrality vis-à-vis that of non-discrimination? Are there further approaches at hand? Is the choice of this meta-technological policy mostly context-dependent, or there is room for some kind of generalization? Should the legal regulation of technology be conceived as an end in itself or should focus be on the social and economical outputs of people adopting a certain technology? How about the alternative between law as meta-technology and techno-regulation? Does the latter inexorably affect the corollaries of the rule of law?

## II. New media and the law

*By Steve Cornelius (University of Pretoria)*

Lister *et al* (*New Media: A Critical Introduction* 2009:32) explains that the mass media which developed during the 19th and 20th Centuries were centralised, content was produced in highly capitalised industrial locations such as newspaper printworks or Hollywood film studios. In broadcast media, press and cinema, distribution was tied to production, film studios owned cinema chains, newspapers owned fleets of distribution vans, the BBC and other national 'broadcasters' owned their transmission stations and masts. Consumption was characterised by uniformity: cinema audiences all over the world saw the same movie, all readers read the same text in a national newspaper, we all heard the same radio programme. And we did these things at the same scheduled times. Twentieth-century mass media were characterised by standardisation of content, distribution and production process.

These tendencies toward centralisation and standardisation in turn reflected and created the possibility for control and regulation of media systems, for professionalisation of communicative and creative processes, for very clear distinctions between consumers and producers, and relatively easy protection of intellectual property. This provided an environment in which governments and

large multinational media houses could determine the social dialogue through selective release of information and carefully constructed entertainment.

New media, though, is dispersed and pervasive. The audience has become fragmented and differentiated and there is a proliferation of media offerings that can be accessed in multifarious ways. Sophisticated camera equipment and remote control drones have become reasonably compact and inexpensive and anyone with a mobile phone can nowadays virtually immediately distribute images from a multitude of angles or commentary of an event over the internet. The internet provides a node which has obviated the need for expensive transmission stations and masts. And the internet knows no national or regional borders.

As a result, the relative monopoly that governments and media houses have so far had over the collation, production and distribution of information and entertainment, is undermined by an overwhelming number of content providers and content distributors. It has become virtually impossible to control the production and distribution of information. In addition, the ability to reproduce material and equipment capable of intercepting broadcast signals are also generally available with the result that it is not very difficult to distribute images on the internet without the knowledge of the producer or broadcaster so that protection of intellectual property becomes much more complex.

Consequently, current models for the regulation and protection of the media have become outdated and needs to be revised. A system of localised management and protection is no longer viable. There is an urgent need for substantive law reform in which a more globalised approach to the media should be established and in which the various roles of the established mass media and the dispersed new media can both be recognised and adequately protected.

## III. To forget or not to forget: that is not the question.

*By Claudio Lucena (Catholic University of Portugal)*

Nearly two years ago the European Court of Justice (ECJ) decided that, in certain circumstances, search result links should be made unavailable for the general public[1], a procedure which should be developed and implemented by search engines themselves[2]. The ruling was already directed specifically to a digital environment, where effects more often than not cross the borders within which a court exercises its jurisdiction. Since the impact of the position of the European Court can and has been felt in different parts of the globe, what since then has been referred to as *the right to be forgotten* is the object of worldwide discussion. The terminology is clearly misleading, and this is but one of the many controversies that flourish about such a legal construction. The issue, which initially seems to address the protection of a personality right to informational self-determination, also presents evident transnational repercussion and raises concerns over other legally protected interests such as Internet fragmentation, freedom of speech, right to information, and in edge situations, memory and history.

Some jurisdictions, pressed by constitutional and legal tradition constraints, still strive with the very anatomy, the elements, the justification and the nature itself of the structure, denying its very concept or refusing to admit its existence or at least some of its repercussions. Others have simply moved ahead towards its implementation in their internal orders. In those, as the original Court decision confirmed that requests to delist can be addressed directly to the search engine itself, such undertakings face the need to develop and implement a proper procedure to comply with the new demand.

First reports released by Google on the matter unleashed strong external criticism as to the transparency and independent oversight aspects of the procedure. These are important features in the discussion, due to public interest

---

1 Case C-131/12, Google Spain v. AEPD and Mario Costeja González [2014] ECLI:EU:C:2014:317, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=firs t∂=1&cid=53949

2 CNIL Commission Nationale de l'informatique et des Libertés. Droit au Deferencement. Interprétation commune de l'arrêt de la CJUE, Republique Française, 2014 http://www.cnil.fr/fileadmin/documents/Vos_libertes/Droit_au_dereferencement-Interpretation-Arret.pdf

values embedded in legal tests to be applied when deciding about delisting, following the Court's established criteria. Companies exploring Internet search as economic activities complain about the new burden which was brought upon them, carrying complex and costly public interest duties to handle.

It is in this given context that unconventional multistakeholder governance models which have grown in importance and presence in the last decade, structures that are meant to involve players beyond traditional ones, in an attempt to widen the scope of their representation and legitimacy, are contributing to build a new way of debating, proposing, designing and implementing policy and will be further explored in this work as a possible way to provide existing legal frameworks adequate tools to enhance transparency, compliance-monitoring and enacting requirements.

This work presents the legal discussion concerning the obligation to delist links from search engines with its basic requirements, draws a brief snapshot of the current situation in the world, then focuses on the terminological discussion, pointing out the inadequacy of the terminology largely adopted by international press and even policy bodies themselves, and stressing the various pitfalls into which the use of the misguiding terminology can lead. Finally, the workt tries to discuss and propose multistakeholder efforts and initiatives to build an enforcement system which responds better to a reality that demands this involvement from these private information and data agents, and which has to place them under new standards of accountability[3], yet to be debated and developed.

## IV. Artificial reproductive technologies and international law: the role of human rights

*By Ludovica Poli (Turin University)*

3 Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data. May 14, 2015. https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd#.fscz35uy1

The paper aims at exploring the role of international human rights law in regulating new technologies applied to the beginning of human life. It first considers bioethical divisive issues arising from the application of artificial reproduction technologies (ART) (par 2) and their relevance in the human rights (HR) debate (par 3). The analysis then moves to consider more in details the contribution of international human rights law in regulating these new technologies, both in the perspective of the law making process (par 4) and of the law interpretation by international HR Courts (par 5). With special reference to the case-law of the European Court of human rights (ECtHR), the Author argues that, through argumentative *escamotages*, the Court constantly expresses a human rights oriented position, playing a key role in ruling on new technologies (par 5 1; 5 2). The study finally demonstrates that legal reasoning of the ECtHR represents the field where bioethics meets human rights law: as a matter of fact, international courts makes distinct ethical choices, rather than having a neutral voice in regard to the bioethical debate underpinning each case (par 6).

Whenever a bioethical dilemma arise from actual facts, it first requires to be qualified in terms of rights of people involved. As it usually implies a request from an individual to the state, this triggers a HR approach in solving the issue. While this approach might not provide a sound result, it certainly helps to identify all the relevant subjects involved in the bargaining for a solution. The main contribution of human rights in the bioethical debate is precisely the identification of all the relevant subjects and interest involved. These includes not only existing individuals, but also future generations and - to a certain extent - potential individuals, as well as various collective interests (public moral, public health…)[4].

Once defined the competing interests at stake, any (international) judge called to decide a case, will need to find a correct balance among rights. An operation of this kind necessarily leaves some space for discretion and, more

[4] This argument is in line with the idea of those Scholars who 'see human rights discourse as a way of posing questions and setting up problems for analysis and resolution, even where they do not see human rights as a useful set of theoretical tools for that analysis or for defining solutions to moral and political problems': Schroeder 'Human Rights and their Role in Global Bioethics' 2005 *Cambridge Quarterly of Healthcare Ethics* 221; Thomasma 'Proposing a New Agenda: Bioethics and International Human Rights' 2001 299 (both quoted by Aschroft, *supra* n 64 at 40).

importantly, implies an ethical approach: a reasoning aiming at finding an ethical solution, conforming to a standard of what is right and good. As it was correctly stated by DEMBOUR, 'the real work starts, rather than finishes, where the Court agrees that a particular right is engaged. For that is the point at which ethical argument is required in order to deploy concepts of balance, proportionality, margin of appreciation, and so on'[5].

HR Courts, and the ECtHR in particular, play thus a prominent role in ruling on new technologies applied to the beginning of life and, in doing so, express ethical stances capable of influencing the moral debate on divisive topics.

## V. Threats of the internet of things in a techno-regulated society: A New Legal Challenge of the Information Revolution

*By Eduardo Magrani (FGV Law School in Rio de Janeiro)*

Technology has been rapidly changing the way we interact with the world around us. Companies, aiming to meet new consumer demands, are developing products with technological interfaces that would have been unimaginable a decade ago. Automated systems turn on lights and warm meals as you leave your work, intelligent bracelets and insoles share with your friends how much you have walked on foot or on bike[6]; sensors that automatically warn farmers when an animal is sick or pregnant[7]. These examples are all manifestations associated with the concept of "Internet of Things" ("IoT").

There are strong disagreements regarding what IoT stands for. There is no such thing as a unanimously well-defined concept for IoT. More broadly, it can be understood as an interconnected environment of physical objects linked

[5] Dembour *Who Believes in Human Rights? Reflections on the European Convention* (2006), quoted by Aschroft, *supra* n 64 at 40.

[6] Nike Running. "The New Nike+ Running App" *YouTube*. YouTube, 26 June 2012. Web. 16 March 2016.

[7] Computer Science Zone Security and the Interent of Thing, available from http://www.computersciencezone.org/wp-content/uploads/2015/04/Security-and-the-Internet-of-Things.jpg#sthash.c6u2POMr.dpuf

to the Internet through small built-in sensors, that creates a computer-based ubiquitous ecosystem, in order to facilitate and introduce functional solutions for daily routines and activities[8][9].

Even though it might resemble a futuristic scenario, this kind of technology is already part of the present. Bracelet computers, smart watches, health devices, smart houses, cars and smart cities, are all manifestations of the "Internet of Things". [10]

However, despite the present context, it is still a fairly recent culture based on the new relations we are forging with machines and interconnected devices. It is estimated that the number of "things" connected to the Internet have surpassed the number of people, what further confirms this new human-machine relationship. Estimations [11] tells that in 2020 the quantity of interconnected objects will overcome 25 billion, being able to reach a mark of 50 billion of smart devices.

All this hyperconnectivity and continuous interaction between gadgets, sensors and people, points to the rise of data and logs being produced, stored and processed both virtually and physically. On one hand, this may produce innumerous benefits to consumers. Interconnected health devices allow constant and efficient monitoring as well as greater interaction between doctor and patient. Residential automated systems will enable users to send messages to their home devices even before they arrive, performing actions such as opening the garage door, turning off alarms, turning on the lights, preparing a hot bath, cooking dinner, playing that special song, and even shifting the rooms` temperature. Moreover, what the future holds for IoT is yet to be discovered.

On the other hand, the large amount of connected apparatuses will accompany us daily and regularly in our everyday life, and therefore collecting, transmitting, storing and sharing an enormous amount of data – most of it strictly private and even intimate.

---

[8] FTC Staff Report Internet of Things: privacy & security in a connected world (2015)
[9] NICbrvideos. "A Internet das coisas, explicada pelo NIC.br" *YouTube*. YouTube, 16 July 2014. Web. 16 March 2016.
[10] FTC Staff Report (2015)
[11] *ZDNet* (2014-11-11). Available from http://www.zdnet.com/article/25-billion-connectedd-devices-by-2020-to-build-the-internet-of-things/.

With the exponential rise of such devices, we should also pay attention to the potential risks and challenges that this increase may bring to fundamental rights. Those challenges can be investigated through a wide variety of lenses. For example, the new technological scenario is occasioning several changes on regulation and in jurisprudence of consumer's law. Nevertheless, despite the variety of areas covered by this discussion, the analysis intended in this paper will try to investigate those challenges especially through the lens of privacy, freedom of expression and protection of personal data.

Although some of the threats and risks of the IoT scenario do not seem novelty, considering how recent this context of hyperconnectivity is, we are not yet fully conscious of the possible damages that are dramatically enhanced in an IoT environment nor do we have sufficient legal regulation to avoid losses that could arise from the unclear processes of storage, treatment and sharing of our personal data in a context of IoT.

Besides, while we are failing on having an adequate regulatory framework upheld by the law, we are experiencing a strong auto-regulation from the market, a regulation that, at many times, is made through code design[12], what we may call a "techno-regulation". It is crucial to analyze what are the new legal challenges in this context that forces us to think about an adequate legal framework to respond to those challenges.

With that in mind, this paper is structured in two main sections. The first introduces the concept of IoT as well as shows how the focal point of this discussion goes beyond the IoT itself, linking up to the concepts of interconnectivity and Web 3.0. To reflect on the IoT nascency, it is important to take a step backwards and look carefully into the impacts of (the promise of) hyperconnectivity. That is why the next section, even though titled "The Internet of Things", is not restricted to IoT, it encompasses the development of the Web –

[12] The expression "code design" here refers to the architecture of technology encompassing not only software though algorithmic design but also hardware architecture, as stated by Lawrence Lessig. "This regulator is code--the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced." LESSIG, L. Code Is Law: On Liberty in Cyberspace. (2000). Available from http://harvardmagazine.com/2000/01/code-is-law-html.

showing how the user's experience has changed in a context of greater interactivity and connectiveness.

The second section of this essay tries to sustain the importance that the law advances in the search for a new regulation, especially in Brazil, that is both adequate to new technologies and that fits the new IoT context, preventing a negative scenario where the techno-regulation overlaps the regulatory framework based on the rule of law and controls us in an insurmountable way, potentially violating several fundamental rights.

Based on a theoretical and constitutional approach to current technological evolution with particular regard to the Internet of Things and its privacy dimension, the purpose of this preliminary effort is to trigger further reflections about the regulatory challenges posed by greater (inter)connectivity.

## VI. Smart Cities: Technological Opportunities and Legal Challenges in Developing the Internet of Things for Public Goods

*By Alexandre Pacheco da Silva and Rodrigo Moura Karolczak (FGV Law School in São Paulo)*

Kelsey Finch e Omer Tene[13] state that, during the 1960's, the American urban planner Jane Jacobs challenged the first wave of urban restructuring policies applied in North American cities. She claimed that such policies understood all cities based on a single urban planning model, ignoring local necessities and regional characteristics from the regions in which the cities were located.

The project of the single, modern, standardized and technological city was based on the perception that it would be possible to create a specific design which broadly supplied to the offer of services for North American citizens, based on a model of organization of the local administration that considered the challenges of modern life. There was a strong association between a certain

[13] Finch; Tene "Welcome to the Metroptiocon: Protecting Privacy in a Hyperconnected Town" 2014 Fordham Urb. L. J. 1581-1582.

model of city and the understanding that such model would result in inevitable progresses, based on the technological promises for such cities[14].

Jacobs criticized the compartmentalization of the urban areas, organized by "zones" (residential, industrial and commercial), and defended a more integrated city model, with shared spaces capable of creating different levels of interaction between citizens. In Jacobs's view, the use of technology should allow for a higher level of integration between urban areas, and not for segregation of separate areas, each one representing different "moments" of life: the "industry-work", "residence-leisure" and "commerce-consumption" [15].

Nowadays, once again, the debate regarding transformations on urban infrastructure based on a new technological scenario reaches urban planners, entrepreneurs, developers, scholars, policy makers and ordinary citizens, now under a new terminology of "smart cities", with the purpose of integrating smart communities into more connected, efficient, sustainable cities, and with better quality of life.

Guided by the technological promises of the Internet of Things – IoT, alongside Big Data and Cloud Computing technologies, the smart cities initiatives have also been surrounded by euphoria, without, however, a clear analysis over the real contribution of these technologies for the improvement of smartness in cities[16].

The concept of smart cities is currently associated with the cities' capacity of achieving the provision of better public services based on a better understanding over what their citizens wish and how they behave. Cocchia[17] states that the definitions often used by scholars for smart cities define quality of life in a way which is "linked with the quality of people and community, depending on the cultural level, the data information and knowledge sharing, but also some other aspects of community life".

---

[14] Finch; Tene 2014 Fordham Urb. L. J. 1582.
[15] Jacobs The Death and Life of Great American Cities (1992).
[16] Finch; Tene 2014 Fordham Urb. L. J. 1582.
[17] Cocchia Smart and Digital City: A Systematic Literature Review (2014) in Dameri; Rosenthal-Sabroux Smart City: How to create public and economic value with high technology in urban space 31.

For instance, the city of Tallinn, in Estonia, has created an investment program in 2008 for the development of a technological infrastructure[18] based on information and communication technologies for the management of traffic, school enrollments, tax collection and relationship with the citizens. This initiative required professional training activities to operate the infrastructure with investment in technical schools and higher education institutions geared to the development of technologies with special focus on cities.

Even preserving its medieval architecture and the structure of public buildings of the former Soviet Union, the city has become a reference for the debate over smart cities, mainly for being the hometown of Skype[19]. Nowadays, Tallinn residents rely on internet connected devices to access practically all of the city's public services. Through their *smart ID cards*, they are capable of accessing the public transport system without any cost, and the city council is able to monitor the volume of users who are using the services in real time. The areas of the city which are available for car parking also require the insertion of codes electronically provided by the local transit authority, and the user receives the electronic vouchers for payment sent by the city council within a few hours.

From 2008 to 2012, the city has channeled 80% of all direct foreign investment of the country on information technology projects, being responsible for the development of one of the most advanced *smart ID card* technologies ever developed[20]. However, without their *smart ID cards*, Tallinn residents are not capable of accessing the cities' public services, and the public authorities would not be able to identify them as recipients of their services.

---

[18] There are several reports on the development of the technological infrastructure in Tallin. Among the aspects that have been highlighted in this regard is the capacity of integrating the services offered to the public, associated with the construction of an environment favorable for the creation of technology-based start-ups, such as *TransferWise*, *GrabCad* and, mainly, *Skype*. All the attention directed to the city is also a result of its ability of attracting information technology professionals for the country, mainly for the area near the campuses of Tallinn Technical University and Tartu University. Among the most prominent technological solutions in the city is the use of an electronic ID card that allows citizens access to all public services of the city through a unique and interactive system. (Access in: https://www.quora.com/Why-is-Tallinn-considered-a-smart-city).

[19] On February 10 2016, the city of Tallinn was elected one of the smartest cities in the world by the Intelligent Community Forum, a Think Tank located in New York and dedicated to the study on how the creation of technological infrastructures can increase intelligence on cities. (Access in: http://www.npr.org/sections/parallels/2013/06/12/190693661/tallinn-the-former-soviet-city-that-gave-birth-to-skype).

[20] Finch; Tene 2014 Fordham Urb. L. J. 1582.

When addressing the new legal challenges arising from the advancement of the Internet of Things (IoT), Weber states[21] that even if the IoT is capable of bringing profound transformation on contemporary societies, there are no efforts for the creation of a regulatory framework capable of dealing with the problems related to the expansion of use of personal data for the creation of smart cities. The wide exchange of data between devices and the incorporation of such data on the autonomous decision making by computerized systems has resulted on questions regarding the citizen's privacy in this new environment, as well as the potential security risks in the control of connected devices.

Therefore, this article aims to discuss how the debate over smart cities has been influenced by the introduction of the IoT, in particular by contrasting the opportunities that the IoT has created for the enhancement of smartness in cities with the necessity of creation of a legal standard for data protection inserted on the new dynamic of collection, treatment, sharing and storage of data required by the IoT.

Our goal is to provide a broad picture of the opportunities and the challenges created by the increasing use of IoT technologies in the construction of smart cities, and how this phenomenon may contribute to the improvement on management and planning on contemporary cities[22].

---

[21] Weber "Internet of things: Privacy issues revisited" 2015 Computer Law & Security Review 619.

[22] This set of issues on public policies aided by information technology relates to the debate on Digital Democracy, or Internet and Policy, which seeks to understand the digital citizen's participation on government decision-making and on the accountability of democratic rule of law in a computerized society. Gomes Participação política *online*: questões e hipóteses de trabalho (2011) in: Maia; Gomes; Marques (orgs.) Internet e Participação Política no Brasil 27-28. An important definition in this field is established by Gomes, who states: "What I understand by digital democracy is any form of use of devices (computers, smart phones, palmtops, ipad...), applications (software) and tools (forums, websites, social networks, social media ...) of digital communication technologies to supplement, enhance or correct aspects of political and social practices of the state and citizens, for the benefit of the democratic content of the political community." However, it is important to highlight that part of the debate understands that not only the positive aspects of on-line political participation are relevant, but also the political disputes conducted on the on-line environment. Coleman; Blumler The Internet and Democratic Citizenship: Theory, Practice and Policy (2009) 7. Coleman and Blumler point to different types of political citizenship that are also expressed on-line, effectively challenging the acts of the state. For the authors, "at some times political citizenship is defined in terms of the state's requirements for order amongst its subjects, and at others it emerges out of the collective values, voices and actions of the people themselves. Incumbent democracy is served by the former; critical democracy by the latter."

For that, we have structured this work by using the second segment to introduce how the IoT has been incorporated on the debate over smart cities and how it has become a central element of this debate. On the third segment, we demonstrate how this importance is associated to the evolution of IoT related technologies themselves, in order to, ultimately, discuss the legal challenges related to data protection which are present in this process.

## VII. Good governance for consumer welfare and accountability in the age of digital aggregators: The case of Amazon India

*By Sunita Tripathy (Jindal Law School in India)*

Cases of illegal online pharmacies, grey and black marketing through e-commerce channels are on the rise worldwide as also in India. The fundamental basis for e-commerce as such, is that it is entirely consumer-driven. It holds consumer welfare, qualified by convenience and quality-control, dear to its success. Digital aggregators have an intermediary yet crucial role in the online marketplace as they are the ones which bring the buyers and vendors together under one space, generate awareness and enable consumer preference determination. The consumer testimonials, feedback and ratings lead to upgradation of goods and services within sectors; thereby fostering competition between vendors which influences pricing of such goods and services.

Digital platforms are not merely spaces which enable payment gateways for the customer but, as noted in the study conducted by the Organisation for Economic Co-operation and Development (OECD), they may provide a range of often bundled services such as 'fixing prices, transaction processing and co-ordination, quality guarantees, monitoring, as well as, in some cases, stock management.'23 Consequentially, digital aggregators can be identified not only as online 'market creators' but also ones who maintain the market so created.

---

[23] The OECD Study on "Economic models and role of Intermediaries in the Value Chain" (April 2010) available online at : http://www.oecd.org/internet/ieconomy/44949023.pdf (accessed on June 12, 2015).

The consumer's decision to purchase any good or service online is often based on his/her confidence in the digital aggregator's brand name.24 Therefore when a consumer receives a delayed delivery or a fake product, or when the brand does not honour the warranty for such deficiency in service, concerns related to accountability arise.

The Indian Courts are yet to determine the liability, if any, of a digital aggregator operating via a third-party marketplace model. The Division Bench of the Delhi High Court has in the matter of World Wrestling Entertainment, Inc v. M/s Reshma Collection (decided on October 15, 2014) conclusively held that "jurisdiction in e-commerce cases involving trademark and copyright disputes would be determined by the **buyer's place of residence**"25 thereby reiterating that the convenience of the end-user is the most important goal of any service industry.26

---

[24] Conclusively, vendors also choose to list themselves with such digital aggregators, rather than sell through their own portals because of the robust online infrastructure in the nature of the e-commerce website made available by Amazon like digital aggregators and also because of the tremendous reputation enjoyed by such brand.

[25] FAO (OS) 506/2013, Delhi High Court, 15 October 2014. See, judgement here: http://indiankanoon.org/doc/71641182/ (accessed on June 12, 2015); The Division Bench relied on the judicial reasoning in the landmark case of Bhagwandas Goverdhandas Kedia v Girdharilal Parshottamdas & Co., AIR 1996 SC 543, and reiterated that while the general rule of acceptance of any contract being that, the contract is complete when the offeror receives intimation that the offeree has accepted his offer; the exception to this general rule is when the contracts are negotiated by postal communication or telegrams, the contract would be said to be complete when the acceptance of the offeree is put into a course of transmission by him/her by posting a letter or dispatching a telegram. In the Bhagwandas case the Supreme Court had held that offer and acceptance via instantaneous communication such as telephonic conversation would not attract the exception to the general rule of contract. See also, Devika Agarwal, "Jurisdiction in E-Commerce IP Disputes" (October 18, 2014) available online: http://spicyip.com/2014/10/jurisdiction-in-e-commerce-ip-disputes.html (accessed on June 02, 2015). Further the Court observed that the catalogued list of goods and services on an e-commerce website constitute an 'invitation to offer' while the consumer's order to purchase any goods and services so displayed constitute 'an offer' to buy. When a consumer who is based in Delhi, successfully makes a purchase through confirmed e-payment that is when the offer to buy is said to have been accepted by the online vendor. As this transaction takes place instantaneously, the communication of acceptance by the online vendor is also said to be instantaneously communicated to the consumer through the internet at Delhi. Therefore, it is considered that the essential part of the vendor's business is being carried out at Delhi.

[26] Reliance was placed upon the Supreme Court's three-pronged test laid down in the matter of Dhodha House v. S. K Maingi (2006 (9) SCC 41) to determine the appropriate forum for litigants, and the interpretation of the expression '***carries on business'*** as entailed in Section 134 (2) of the Trade Marks Act, 1999 and Section 62 (2) of the Copyright Act, 1957 to mean that a person may not necessarily carry out the business by himself but may do so even through a servant or **an agent**. The conditions set out by the Court include: (i) The agent must be a special agent who attends exclusively to the business of the principal and carries it on in the name of the principal and not as a general agent who does business for anyone that pays him; (ii) The person acting as

For the purpose of addressing the possibility of law evolving as a meta-technology to ensure that the digital aggregators who are drivers of e-commerce be encouraged to take a proactive role rather than a defensive role in containing the illegal activities of its vendors and participate in devising robust industry regulatory mechanisms that minimize aberrations leading to consumer exploitation on the part of such deviant vendors, the marketplace model of one such Indianized27 digital aggregator, which enables third party vendors to reach consumers, namely Amazon India is discussed herein as a case study.

## VIII. A Consumer's Case for Regulating Electronic Credit and Debit Transfers (EFT's) in South Africa

*By Sylvia Papadopoulos (University of Pretoria)*

The use of electronic payment systems is actively encouraged by financial institutions because they are cost effective; facilitate transactions with ease and speed, facilitating a more competitive market through an expanded customer choice.[28]

According to the OECD there are two core issues that should be taken into consideration by regulators to strengthen consumer protection for users of these payment systems, firstly that there should not be differentiated levels of

---

agent, must be an agent in the strict sense of the term and a manager of a Joint Hindu Family cannot be regarded as an agent within the meaning of this condition; and (iii) To constitute carrying on business at a certain place, the essential part of the business must be performed at that place. As the Appellant did not have any 'agent' in Delhi, the Hon'ble Division Bench went ahead to examine if the third condition was being fulfilled in the instant case, i.e., whether an essential part of the Appellant/Plaintiff's business was being performed at Delhi. To determine this, the Court invariably dealt with the question of where a contract is concluded when the transaction takes place over the internet.

[27]Amazon.com, Inc. is a NASDAQ-listed American electronic commerce company with headquarters in Seattle, Washington USA and has operationalized an Indian Franchise named Amazon India. According to Michael De Kare-Silver "Amazon has 175 million active accounts worldwide and that has led to $75 billion in global revenues", *see* Digital Insights 2020: How the Digital Technology Revolution is Changing (Leicestershire, England: Troubador Publishing Ltd, 2014) at 101.

[28] Perlman (2012) LLD 18; Baxter (1974) *Univ of Toronto LJ* 63.

protection, such as limitations on consumer liability, between different access devices used to initiate payment over electronic payment systems (at present credit cards offer the best chargeback mechanisms and protection from fraud losses) and secondly regulators should ensure that there are minimum levels of payment protection for all payment services.[29] This is currently not the case in South African jurisprudence. From a consumer protection perspective one of the most problematic areas of payment services is the electronic fund transfer (EFT).

When using an EFT to facilitate payment to a third party the question that arises is when is the payment complete and therefore final and irreversible? This is important if for example a consumer wants to revoke a payment instruction, recover mistaken or fraudulent EFT's, where death, winding-up, liquidation or sequestration terminates the authority/mandate to pay and where payment is required on a specific date.[30]

South Africa does not have dedicated legislation for electronic payments like the European Union's Payment Services Directive,[31] and the limited available positive law around this issue is problematic. The consumer (who is actively encouraged to use EFT's) carries a disproportionate amount of risk and when they resort to litigation it does not produce consistent results, as this article will primarily articulate. This is in direct contrast to the European Union who have provided a legal foundation for payment services across the EU since 2007. The Payment Services Directive (PSD1)[32] aimed to ensure more transparency and information for consumers, strengthen refund rights and clarify the rights and duties of consumers and payment institutions. In July 2013 the EU Commission

---

29 OECD's *Report on Consumer Protection in Online and Mobile Payments* (2012) 5 and 35.

30 Geva (2008) *Chicago-Kent Law Review* 633-634.

31 The Directive on Payment Services 2007/64/EC (PSD1) will be repealed on 13-01-2018 by Article 114 of the new Directive 2015/2366 of The European Parliament and of The Council of 25 November 2015, On Payment Services In The Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, (hereafter PSD2) which took effect on 12-01-2016. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366 >(accessed 15-05-2016). Article 115 states that by 13 January 2018, Member States shall adopt and publish the measures necessary to comply with PSD2.

32 The Directive on Payment Services 2007/64/EC (PSD 1) which is set to be repealed by the Revised Directive on Payment Services (PSD2) adopted by the European Parliament on 08-10-2015 see http://www.europarl.europa.eu/news/en/news-room/content/20151002IPR95307/html/Opening-up-the-online-payments-market-so-as-to-reduce-fees-and-fraud-risks (accessed 15-10-2015).

decided to revise PSD1 so as to modernise it by taking into account new types of payment services and innovation in the industry. The main objectives of PSD2 are to contribute to a more integrated and efficient European payments market, level the playing field for payment service providers, make payments safer and more secure, protect consumers and encourage lower costs.[33] Mindful of the pitfalls of any comparative exercise, this article sets a secondary aim of explaining how the European Union is addressing the issues of refund rights for consumers, the rights and duties of consumers and payment institutions alike within the electronic payments arena.

## IX. Regulation of Uber in São Paulo: from conflict to regulatory experimentation

*By Rafael Zanatta and Beatriz Kira (FGV Law School in São Paulo)*

Uber is a company founded in San Francisco (USA) that offers the consumer an individual transport option with three important innovations: (i) race call through global positioning system (GPS); (ii) payment methods via smartphones, and (iii) reputational system where drivers and passengers are evaluated after the race. In May 2014, the company started its operations in Rio de Janeiro, and in June 2014 the company started operating in the city of São Paulo – the biggest city in Brazil, with more than 14 million people. The entry in Brazil occurred in a global scenario of taxi drivers protest against "illegal" and "unfair competition" because Uber is not registered as a transportation firm.[34]

Legal responses to the emergency of the so-called "transportation network companies"[35] are many and varied because of local legal culture, the

---

[33] European Commission Fact Sheet on the Payment Services Directive (hereafter PSD2 Fact Sheet), 08-10-2015, par 1-3 available at http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en (accessed 18-05-2016).

[34] Geradin 'Should Uber be allowed to compete in Europe? And if so how?' 2015 *George Mason University Legal Studies Research Paper Series*.

[35] Zanatta, De Paula & Kira *Inovações Regulatórias no Transporte Individual: o que há de novo nas megacidades após o Uber?* (2016) 9.

power of mobilization of taxi drivers, and policy coordination capacity of new technology companies. The responses also vary from *judicial* - court decisions motivated by petitions and legal battles articulated with lawyers -, and *legislative* - regulatory initiatives by lawmakers or transport authorities.

We discuss in this article the specific context of the entry of Uber in the city of São Paulo during the years of 2014 and 2016. We adopt a socio-legal approach to study the legal tensions between the actors involved in the conflict around the legality of new tech firms in the field of transportation. We organized our narrative in three periods. The first is the short period in which workers and associations mobilized resources to ban Uber at the municipal level. The second period is the moment when legal battles began and both sides (taxi drivers and Uber) hired lawyers to obtain legal opinions to fight at Courts. The third period is the one in which the City Hall begins experimenting a new approach on regulation and the legal complexity on the issue increases.

Our study reveals the tensions behind the "experimental regulation"[36] in São Paulo, which was not tested on a small scale and is not directly inspired in any other regulation around the world. We also show the increasing number of social actors involved with this regulatory process and the growth of legal instruments used to either block or allow this type of firm in Brazil. Finally, we discuss how this methodology can be applied for comparative socio-legal studies and how we might compare the regulatory experience of São Paulo with other major cities around the world.

## X. A human rights perspective on autonomous weapons in armed conflict: The rights to life and to dignity

*By Christof Heyns (University of Pretoria)*

Traditionally, weapons users have been in direct physical control of their weapons. Over the years, revolutions in military affairs have produced weapons

[36] Heilmann 'Policy experimentation in China's economic rise' 2008 *Studies in Comparative International Development* 5.

with increased range and fire-power, but by and large, this did not change the fact that the person activating the weapon took the decision when and against whom force would be used, while being present on the spot from where force was projected.

The advent of unmanned or human-replacing systems has meant that the person launching the weapon no longer needs to be physically present at the time and place from where it is released. The first generation of these unmanned systems are remote controlled weapons systems. The best-known iteration of this technology, armed drones, allow their users to be half-way around the world in a control room when pressing a button that releases a missile from a weapon platform hovering above the target.[37]

The emphasis of this article is on the next generation of unmanned systems in armed conflict. So-called "autonomous weapons" (sometimes simply called robots or machines, or "killer robots") would allow for the release of force from unmanned systems that are no longer remotely controlled by humans.[38] Instead, once a human has activated an autonomous weapon system, on-board computers will make the determination, independent from direct human intervention, on when to release force and against whom it should be directed. Humans remain in the wider decision-making loop, but computers control the critical functions – the release of force. It is not a human being but a computer who "pulls the trigger".[39]

The "autonomy" of robots is not comparable to the autonomy of human beings, which is often seen as the basis of the ability of humans to act as free moral agents. However, robots with a high level of autonomy can perform

---

[37] Peter Singer, *Wired for War: The robotics revolution and conflict in the 21st Century* (Penguin, 2009) p. 179 and further, notably p. 203.

[38] Autonomous weapon systems are platforms, to which any weapons may be fitted. In armed conflict the weapons used are as a rule lethal - hence the term Lethal Autonomous weapons or Autonomous weapons is sometimes employed in this context. If they are to be used in law enforcement, less lethal weapons may be fitted to an autonomous weapon platform. "Autonomous weapons" is thus an umbrella term that serves to cover its use during armed conflict as well as law enforcement. Using this more inclusive term helps to emphasise that some of the same issues arise in both situations, and that these weapons should not only be dealt with as a disarmament matter.

[39] For a discussion of the definition of autonomous weapons, see Michael Schmitt 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) *Harvard National Security Journal Features* 3-7.

functions that those who programme or deploy them cannot foresee (and in that sense, loosely speaking, autonomous weapons have something comparable to "free will"). They are not merely "automatic" and as such respond in predictable ways to a predictable environment – they are "autonomous" and can thus respond to an unpredictable environment, in sometimes unpredictable ways. This is because machine learning takes place (they alter their behaviour based on their experience). Moreover, especially in the context of something as chaotic as war, not all scenarios can be foreseen and provided for. As such they can potentially undermine or limit human autonomy and control over the world.

The advent of autonomous weapons has made it possible for humans not only to be physically absent from the point of release of force, as with armed drones, but to be psychologically absent as well, to the extent that they do not take the on-the-spot decision to direct and open fire. The actual release of force may take place elsewhere and some time after the system was activated. There is thus a process of increasing depersonalisation in the use of force through unmanned systems – already present in the case of remote-controlled weapons, but taken to the next level with autonomous weapons.

It should be emphasised that what is under discussion here is the release of force against human beings. Autonomous weapons may also be used against objects, or incoming munitions, but such a scenario does not raise the concerns addressed here.

While earlier revolutions in military affairs gave the warrior control over ever more powerful weapons, autonomous weapons have the potential to bring about a change in the identity of the decision-maker. The weapon may now to some extent become the warrior.

According to philosopher Nick Bostrom, the appropriate response of human beings to the advent of artificial intelligence is the central question of the day.[40] Autonomous weapons represent this question perhaps in its starkest form. In the context of a more general concern about the role of computers in the world of the future, the significance of the possibility that they may soon be able to forcibly end human life is clear. If they hold the key to human life and death,

[40] Nick Bostrom *Superintelligence* (OUP 2014).

the question could be asked, on what principled basis can their their increased control over other aspects of our lives be resisted?

From what normative perspective can this issue be assessed? An important perspective would be the one of human rights. Human rights are widely accepted as the dominant normative – ethical and legal - framework of the international community. Seen in that light there appears to be value in asking what the implications of the dominant normative framework of our time are for the central question of the day.

To the extent that the human rights framework has been used to address this question, the focus has often been on the right to life implications of failures by autonomous weapons to do proper targeting.[41] I believe this is the right starting point, but further perspectives may be gained by focussing also on another central right potentially implicated by autonomous weapons, namely the right to dignity. The rights to life and to dignity are core constuent parts of the human rights project as we know it today.

Hopefully, a reflection on autonomous weapons from the perspective of these two central rights in this rather dramatic context could also provide some pointers for our relationship with technology on a broader scale.

The potential advantages of autonomous weapons should be recognised. They do not only offer potential military advantages to those who deploy them, but they may – so it is claimed – under certain circumstances also ensure better targeting, and as such save the lives of civilians who are not engaged in the conflict. It is on that basis that roboticist Arkin and others has defended the development and use, under certain circumstances, of autonomous weapons.[42] They have the ability to take but also to save lives. Clearly, neither from a military nor a human rights point of view can such potential capabilities be dismissed out of hand. To what extent is it possible to ensure that the benefits offered by autonomous weapons are used but its disadvantages are avoided?

---

[41] See for example Human Rights Watch *Shaking the foundations: The human rights implications of killer robots* (2014) 5 Available at http://www.hrw.org/reports/2014/05/12/shaking-foundations.

[42] See Arkin, RC 'Lethal autonomous systems and the plight of the non-combatant' (2014) Ethics and Armed Forces 9.

I presented some of the questions raised by autonomous weapons in a report to the United Nations Human Rights Council in 2013.[43] At the time, I argued that states should impose national moratoria on the development and use of autonomous weapons until such time as an internationally acceptable way of dealing with increased autonomy in targeting has been found. In the meantime, the global engagement with this issue has advanced to the point where it may be easier to come to a firm view. This issue has been taken up in a number of international fora and has been subjected to thorough multi-disciplinary consideration.[44] Eminent scientists have expressed themselves against full machine autonomy.[45] A thorough academic discussion has also taken place.[46]

---

[43] See note 1.

[44] The UN Disarmament Committee; United Nations Human Rights Council; also see the Campaign to Stop Killer Robots at https://www.stopkillerrobots.org/

[45] See 'Autonomous weapons: an open letter from AI & robotics researchers' Available at http://futureoflife.org/open-letter-autonomous-weapons/

[46] See Anderson, K & Waxman, M 'Law and ethics for autonomous weapon systems: why a ban won't work and how the laws of war can' (2013) *American University Washington College of Law Research Paper*; Anderson, K & Waxman, M 'Law and ethics for robot soldiers' (2012)32 *American University WCL Research*; Arkin, R 'Governing Lethal Behaviour in Autonomous Robots' (2009) *International Committee of the Red Cross Press*; Asaro, P '*Jus nascendi*, robotic weapons and the Martens Clause' (2015); Asaro, P 'On banning autonomous weapon systems: human rights, automation, and the dehumanisation of lethal decision-making' (2012) 94 *International Review of the Red Cross* Volume 94 Number 886 (Summer 2012), available at http://www.icrc.org/eng/resources/international-review/review-886-new-technologies-warfare/review-886-all.pdf, at p. 10; Evans, TD 'Note at war with the robots: autonomous weapon systems and the Martens Clause' (2014) 41 *Hofstra Law Review*; Herbach, J 'Into the caves of steel: precaution, cognition and robotic weapons systems under the international law of armed conflict' (2012) 4 *Amsterdam Law Forum*; Kastan, B 'Autonomous Weapon Systems: A Coming Legal Singularity'?' (2013) *University of Illinois Journal of Law, Technology and Policy*; Lewis, J 'The case for regulating fully autonomous weapons' (2015) *Yale Law Journal*; Marchant G et al, 'International governance of autonomous military robots' (2011) XII *Columbia Science and Technology Law Review*; Marra, WC 'Understanding 'the loop': regulating the next generation of war machines' (2013) 36 *Harvard Journal of Law and Public Policy*; Melzer, N 'Human rights implications of the usage of drones and unmanned robots in warfare' (2013) *European Parliament Directorate-General for External Policies*; Sassòli, M 'Autonomous weapons and international humanitarian law: Advantages, open technical questions and legal issues to be clarified' (2014)90 *International Law Studies /Naval War College*; Schmitt, M 'Autonomous weapon systems and

There is a growing view that the dividing line between acceptable and not acceptable machine autonomy is determined by the question whether humans retain "meaningful human control" over force delivery. Where that is the case, autonomous weapons are acceptable, but where there is no meaningful human control – where there is in other words "full autonomy" on the part of the machine – they should be banned.

While the exact contents of the term "meaningful human control" still needs to be determined I find this to be a useful approach. I support the ban on fully autonomous weapons. It would be unrealistic and indeed counter-productive to demand complete human control over every aspect of force delivery, but for the reasons outlined below I think that the retention of a certain level of human control is foundational to the retention of the core values of the right to life and the right to dignity.

The attraction of following the "meaningful human control" route is that it places the extent to which human control or autonomy is retained at the centre, which is the unchanging core, not the level of technology or the kind of weapons used, which will change over time.

In order to address these matters, it is useful to articulate the two primary questions raised by autonomous weapons in the context of armed conflict as clearly as possible.

The first question is to what extent are robots able to make reliable targeting decisions. For example, how well are robots able to distinguish between combatants or fighters and protected civilians? The concern here is

---

international humanitarian law: a reply to the critics' (2013) *Harvard National Security Journal*; Schmitt, M & Thurnher, JS 'Out of the loop: autonomous weapon systems and the law of armed conflict' (2013) *Harvard National Security Journal*; Sharkey, N 'The evitability of autonomous robot warfare' (2012) *International Review of the Red Cross*; Sparrow, R 'Killer robots' (2007) 24 *Journal of Applied Philosophy*; Thurnher, JS 'No one at the controls: legal implications of autonomous targeting' (2012) 67 *Joint Force Q*; Wagner, M 'Taking humans out of the loop: implications for international humanitarian law' (2011)21 *Journal of Law Information and Science*; William, C et al 'Understanding 'the loop': regulating the next generation of war machines' (2013) 36 *Harvard Journal of Law and Public Policy*.

about the right to life of those who may not be targeted, such as protected civilians or wounded soldiers. This is the "Can they do it?" question. It is essentially a practical or technical question and the answer may change as technology evolves. There appear to be distinct limits as to what computers will be able to achieve, for example as far as making value judgements is concerned. At the same time, there seems to be inescapable logic in the contention that robots will over time become better at targeting.

The second question is whether machines, as a matter of principle, should have the power to determine who will live and who will die. This is the "Should they do it?" question. This question brings to the fore right to life issues – is it not an "arbitrary" deprivation of life to be killed by a robot? Here the inquiry is not confined to the right to life of those who are protected – the right to life of those who are legitimate targets also comes into play.

However – and this is often neglected in the discussions so far – the second question also brings into play the issue whether autonomous weapons do not violate the right to dignity of those against whom force is released, whether they are legitimate targets or not, because robots should not have the power of life and death over humans.

To summarise the differences between the two questions that are apparent from the above: The "can they do it?" question is technical in nature while the "should they do it?" question is related to values. Moreover, the implications of the first question are confined to the right to life, while the second can impact on the right to life as well as the right to dignity. Lastly the two questions also differ in respect of the groups whose protection they seek. The first question deals exclusively with the rights of those who are protected from targeting. The second question deals with the rights of everyone in the firing line of autonomous weapons, including those who are not protected by law, such as enemy combatants.

Perhaps the most vexing questions in the context of autonomous weapons – and the one that will be addressed explicitly in the conclusion at the end of the article – relates to the interplay between these two questions. If it is true that fully autonomous weapons can (in some cases, in the future) ensure better

targeting, it means that they can save lives. Are those who are calling for a ban on full autonomy then in effect willing to sacrifice these lives that could have been saved, because using fully autonomy is somehow considered to be wrong?

Clearly, the technical difficulties associated with autonomous targeting will mean that this question can in many cases, for the time being, be brushed aside, by saying autonomous weapons will fail the "Can they?" test, and as a result, the "Should they?" question does not arise. At the same it is a sobering thought that computing power doubles roughly every 18 months.[47]

Those of us who call for a ban on fully autonomous weapons will, in the long run, have to confront the unsettling question why we want them to be banned even if it can be proven that they might save lives. Would banning them under those circumstances not be a violation of the right to life, as opposed to be a way to safeguard that right?

This is the issue that this article wants to address. In order to do this, however, we first need to gain a better understanding of the how the rights to life and to dignity are potentially implicated by autonomous weapons.

## XI. Online copyright infringement, techno-cultural creations and the copyright -technology nexus

*By Caroline B Ncube (University of Cape Town)*

This article discusses how nuanced ways of thinking about copyright and technology may promote more appropriate copyright policy and practice. In particular, it will consider how the principle of technological neutrality may be best deployed to ensure an appropriate regulatory and judicial approach to copyright infringement in the digital environment. This is an opportune time to undertake such an examination as recent case law from Canada[48] and South

[47] See Erik Brynjolfsson and Andrew McAfee *The second machine age* (Norton 2014). 41.
[48] *Entertainment Software Association v Society of Composers, Authors and Music Publishers of Canada*, 2012 SCC 34, [2012] 2 SCR 231; *Rogers Communications Inc. v Society of Composers, Authors and Music Publishers of Canada*, 2012 SCC 35, [2012] 2 283; *Society of Composers, Authors and Music Publishers of Canada v Bell Canada*, 2012 SCC 36, [2012] 326.

Africa[49] has shed light on the principle. The latter case law relates to news aggregation, a technologically driven business model, and is the first judicial articulation of the meaning of fair dealing in South African copyright law. Legislative reform in both countries has raised the question of how to best provide for techno-cultural creations such as User Generated Content (UGC).[50] The appropriate regulatory response to UGC is a question that has seized scholars for a considerable period of time. Some argue that a specific UGC exception is more suitable,[51] whilst others are of the view that the solution is to be found the retention of the status quo combined with business models that allow for effective and simplified licensing.[52] Much thought has been given to how such licensing models might work[53] however a purview of such models is beyond the scope of this article.

This article focuses on Canada and South Africa because they share common historical roots, since both their copyright systems derive from the UK Copyright Act, 1911.[54] Their copyright laws have developed at different paces with the Canadian legislative reforms predating South Africa's recent initiatives. As has been noted, until 2015 South African copyright law had "not speedily responded to the challenges [posed by] the internet, convergence, multimedia, digital technology and e-commerce."[55] South African and Canadian copyright

---

[49] *Moneyweb (Pty) Ltd v Media24 Limited and Another* [2016] ZAGP JHC 81.
[50] Canada's Copyright Modernization Act SC 2012, c 20 and South Africa's Copyright Amendment Bill 2015, Government Gazette No. 39028, 27 July 2015.
[51] Yu "Can the Canadian UGC Exception Be Transplanted Abroad?" (2014) 26 Intellectual Property Journal 177; Chik "Paying it forward: the case for a specific statutory limitation on exclusive rights for user-generated content under copyright law" (2011-2012) 11 John Marshall Review of Intellectual Property Law i; Jamar "crafting copyright law to encourage and protect user-generated content in the Internet social networking context" (2009-2010) 19 Widener L.J. 843.
[52] Slade (2015) "User-Generated Content and Copyright Law: A Business Led Solution?" *Oxford Intellectual Property Research Centre Invited Speaker Series* St Peter's College, University of Oxford [unpublished]; Slade (2014) "User-Generated Content: Copyright as Enabler rather than Obstructer?" *33rd ATRIP Congress* Faculté De Droit De Montpellier - France. 6 - 9 July [unpublished].
[53] Woods "Working toward spontaneous copyright licensing: A simple solution for a complex problem" (2009) 11(4) Vanderbilt J. of Ent. and Tech. Law 1141.
[54] Katz "Fair Use 2.0: The Rebirth of Fair Dealing in Canada" in Geist (ed) *The Copyright Pentalogy: How the Supreme Court of Canada shook the foundations of Canadian copyright law* (2013) 93; Pistorius "The Imperial Copyright Act 1911's role in shaping South African copyright law" in Suthersanen and Gendreau (eds) A Shifting Empire: 100 Years of the Copyright Act 1911 (2012).
[55] Klopper "Copyright and the internet" in Papadous and Snail (eds) *Cyberlaw @ SAIII: the law of the internet in South Africa* 3 ed 2012 137, 168.

laws and judicial approaches are unlikely to progress on an identical trajectory due to their national contexts and constitutional imperatives. As stated by the court in *Moneyweb*:

To start with, our Copyright Act must be interpreted through the prism of our Constitution, the Constitution of the Republic of South Africa, 1996. In order to survive constitutional scrutiny, the Act must be capable of being interpreted in a manner that is consistent with the Constitution.[56] However, it is important to recall that the South African Constitution bears some influences from the Canadian Charter of Human Rights (1982).[57] Therefore, at a basic level, there are also some commonalities in constitutional context. Finally, South African courts have relied on Canadian decisions in the past and in the recently decided *Moneyweb* case.[58]

[56] 54 par 106. Also *see Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International and Another* 2005 (8) BCLR 743 (CC) at para 17.
[57] For a discussion of the relevance of the Canadian Constitution to the drafting of the South African Constitution see Sarkin "The Effect Of Constitutional Borrowings On The Drafting Of South Africa's Bill Of Rights And Interpretation Of Human Rights Provisions" (1998) 1 U. Pa. J. Const. L. 176, 181, 184 – 189.
[58] *CCH Canadian Ltd v Law Society of Upper Canada* [2004] 1 SCR 339 at par 25 (2004 sec 13 (Canlii)) was cited with approval in *Haupt t/a Soft Copy v Brewers Marketing Intelligence (Pty) Ltd* 2006 (4) SA 458 (SCA) 4738-C, par 35 and in *Moneyweb* 4, par 9.