
Threats of the internet of things in a techno-regulated society: a new legal challenge of the information revolution

Eduardo Magrani

School of Law,
Center for Technology and Society,
FGV Direito Rio, Brazil
Email: eduardomagrani@gmail.com

Abstract: The promise of hyperconnectivity. Continuous interaction between gadgets, sensors and people points to the rising number of data being produced, stored and processed. On one hand, it may bring benefits to consumers, on the other, growing connectivity, accompanied by data overflow can also challenge privacy and fundamental rights. This paper approaches some of the challenges faced by the rule of law posed by the advancement of the internet of things, which includes a wide variety of actors, most importantly private companies that seek to promote techno-regulation through design, algorithms and market-based contracts.

Keywords: information revolution; information and communication technologies; ICT; IoT; hyperconnectivity; connectivity; threats; risks; regulation; personal data; fundamental rights.

Reference to this paper should be made as follows: Magrani, E. (2018) 'Threats of the internet of things in a techno-regulated society: a new legal challenge of the information revolution', *Int. J. Private Law*, Vol. 9, Nos. 1/2, pp.4–18.

Biographical notes: Eduardo Magrani is a Coordinator of Law and Technology at the Institute for Internet and Society of Rio de Janeiro (ITS Rio). He is a Senior Fellow at the Alexander von Humboldt Institute for Internet and Society in Berlin, a Professor of Law and Technology and Intellectual Property, a Researcher and Project Leader at Getulio Vargas Foundation (FGV), and the author of the books *Digital Rights: Latin America and the Caribbean* (2017), *Internet of Things* (2017) and *Connected Democracy* (2014). He is a PhD candidate and holds MPhil in Constitutional Law at Pontifical Catholic University of Rio de Janeiro. He is a lawyer, acting actively on digital rights, corporate law and intellectual property fields.

1 Introduction

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

bike¹; sensors that automatically warn farmers when an animal is sick or pregnant.² 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 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.^{3,4}

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 ‘IoTs’.⁵

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. Estimations⁶ tells that in 2020 the quantity of interconnected objects will overcome 25 billion, being able to reach a mark of 50 billion 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 innumerable 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.

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 novel, 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 the 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 design⁷, what we may call a techno-regulation.⁸ It is crucial to analyse what the new legal challenges are 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 IoTs’, is not restricted to IoT, it encompasses the development of the web – 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, such as privacy, freedom of speech and access to knowledge.

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

2 The unravel of the IoT

IoT is a term used to describe connectivity between several internet-sensitive everyday objects – gadgets equipped with sensors capable of capturing details from the ‘real world’, for example temperature, humidity and presence, and sending them to central data stations that collect this information and reuse it in ‘intelligent ways’.

The IoT links the objects of the real world with the virtual world, thus enabling anytime, anyplace connectivity for anything and not only for anyone. It refers to a world where physical objects and beings, as well as virtual data and environments, all interact with each other in the same space and time.⁹

From the perspective of technical standardisation, the IoT can be viewed as 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 (ICT).¹⁰

Connected objects have been part of the discussion since the dawn of information technologies. During the 1990s, Bill Joy, cofounder of Sun Microsystems, spoke about the device for device (D4D) connection, a connection that incorporated not only the net, but also ‘several different webs’.^{11,12}

In 1999, MIT researcher Kevin Ashton proposed the term IoT. Ten years later, he wrote the article ‘The ‘internet of things’ thing’¹³ for the *Radio Frequency Identification (RFID) Journal*, reinforcing the importance of such term. According to Ashton, people will need to connect to the internet in various ways and through different devices due to the lack of time available in the new fast-paced routines. Kevin argues that even our body movements will be stored – with precision and accuracy – as data. The researcher further states that this revolution will be greater than the development of the online world we are familiar with today.

Understanding the conceptual framework behind the evolution of the web versions is crucial to apprehend the sense of hyperconnectivity and interconnectivity as something

that can explain the IoT, although they can be understood separately as different concepts. Hyperconnectivity and interconnectivity are, simultaneously, a temporal relative conclusion and a new market response to old and new societal needs.

According to this understanding, we could say that IoT and the so-called Web 3.0 were created and depend on those new technological potentialities upon which they are supported. Their centrality is based on proposals of new usages through an inter and hyperconnected environment. By depending on hyperconnectivity to promote new uses, IoT and Web 3.0 usages make hyperconnectivity even more intense and needed, stimulating this interrelationship. To clarify the interrelationship between IoT and Web 3.0 we must try to unravel the differences between the different web versions that are usually separated in three stages.

The first web (Web 1.0) emerged during the 1980s and was identified by its potential, connecting people – even though it was restricted to a read-only web. Consumer-producer communication was absent and a characteristic of Web 1.0 but, even though this may sound quite pessimistic and negative nowadays, it did not smoothen the impact of the first web. For the first time, people gained free access to large amounts of information.¹⁴

It is important to note that the term ‘Web 1.0’ emerged after O’Reilly Media started coining and publicising the word Web 2.0 on its’ 2004 conference¹⁵ when arose the need to categorise and differentiate both webs.

The transition process from Web 1.0 to Web 2.0 was unclear. Some websites used resources from both phases, making it difficult to draw the line where Web 1.0 ended and Web 2.0 started. Depending on its purpose, some websites with simple layouts could be as good as the more complex ones. While Web 1.0 was known as ‘the web of knowledge’ due to the rapid increase of info available for those who accessed it, Web 2.0 can be considered as the ‘web of communication’ because of its interactive platforms.¹⁶ The differences between these two phases of the web did not happen because of some great technological innovation, but due to the new ways of using other tools previously available in the same architecture. The two major characteristics of Web 2.0 are its collaborative nature and its constant interaction between users. All these relations were possible due to growing platforms such as social networks, blogs, wikis, and others. With that, content production in the internet started to become more fluid. From the moment users could feed platforms with information, the web became a two-way stream, also labelled as *read-write web*. Therefore, with the advent of the collaborative web (Web 2.0), internet users went from mere content consumers to content consumers and content producers at the same time.

The term Web 3.0¹⁷ was created by the journalist, John Markoff from the *New York Times*¹⁸, based on the evolution of the term Web 2.0 popularised by Tim O’Reilly and Dale Dougherty in 2004.

While Web 2.0 allowed greater interaction, Web 3.0 now uses the internet for massive data crossing. Information can be read through different devices and making it possible for them to deliver precise information. Even though the concept of Web 3.0 remains undefined, fluid and a target for critics, we can still say that some of its characteristics differ from the other webs. The main aspect is the new connection poles where objects interact with people and with other objects – what explains its association with IoT.

The main difference between Web 2.0 and Web 3.0 is the fact that the first focuses on users' creativity for content production, considering both consumers and producers of online information, while the latter (Web 3.0) focuses in interlinked datasets.¹⁹

Below examples of other associations comparing Web 2.0 and Web 3.0.²⁰

Table 1 A comparison of Web 2.0 and Web 3.0

<i>Web 2.0</i>	<i>Web 3.0</i>
Read/write web	Portable personal web
Communities	Individuals
Sharing content	Consolidating dynamic content
Blogs	Lifestream
AJAX	RDF
Wikipedia, Google	DBpedia, iGoogle
Tagging	User engagement

There are those who defend that machine to machine (M2M) connection will be more useful for the organisation of information by the time when personalised and specific data becomes more necessary. This technology, enhanced by greater connectivity between devices, will deliver intelligent and highly customised content. Specialists believe that one of the 'pros' of Web 3.0 and IoT will be its capacity to help in personal assistance while concomitantly learning more from us as we navigate/use it.

Together with the concept of Web 3.0 arose the concept of 'semantic web'. Tim Berners-Lee, creator of the World Wide Web (WWW), explains that semantics is part of the Web 3.0.²¹ During the internet's early days, all content produced was destined for human understanding, for example, all web pages were easily recognisable for us, computer did not possess this ability, but times are changing.

The semantic web implies that devices would be able to interpret information granted and produced by the user. Combining personal information to platforms could further individualise the expected outcomes. For example, even though two individuals may be searching for the same thing using the same terms, different results would be presented to each, because of their online history and individual contexts. Web 3.0, IoT and semantic internet will depend on the large databases that will be created as users further use platforms with this kind of technology.^{22,23}

Beyond the conceptualisation of IoT, another concept rises up closer to the characteristics outlined by Web 3.0 and semantic web: the internet of everything (IoE).²⁴ Companies that work with network infrastructure, such as Cisco and Qualcomm, have been propagating the term in conventions and documents. However, there is no substantial difference between IoT and IoE. Even Qualcomm does not make a clear distinction. On the other hand, Cisco believes that IoT is only a stepping-stone to reach IoE.²⁵

There are already predictions about the next stages of the web. Estimations²⁶ note that the 'Web 4.0' or '5.0' will be a symbiotic web, meaning it will be capable of integrate technologies to humans, even involving feelings and emotions, therefore transforming the web into a brain-like system. The definitions regarding the next webs are openly vague, even the term 2.0 is still a target for critics and the 3.0 is still consolidating. Nonetheless, the possible statements about these new webs point towards greater use of artificial intelligence in order to create an increasingly 'smarter' web.

Taking into consideration the characteristics of the IoT, Web 3.0 and growing (inter)connectivity, in the next topic we will try to shed light on the ongoing challenges faced by the rule of law posed by the advancement of the IoT and the techno-regulation that it imposes capable of limiting and violating several fundamental rights.

3 A techno-regulated society

Considering the characteristics pointed out by cyber-optimistic scholars such as Manuel Castells²⁷ and Yochai Benkler²⁸, we may say that new ICT have been seen as the great promise of several different areas. Nonetheless, this potential can be considerably reduced depending on how new technological layers are built upon certain infrastructures, therefore allowing users to explore more or less actions and depending on criteria for access and content filtering by algorithms.²⁹ Besides, private companies are developing technology without paying adequate attention to fundamental rights such as privacy and security. Without proper care, this procedure can bring serious risks to consumers.³⁰

We are living a moment of intense techno-regulation, commodification of personal data, and no strong legal apparatus to protect human and fundamental rights such as privacy protection. It is crucial that we stop to think about the role that the law should play in this context, especially in countries like Brazil that don't have yet for example a solid and comprehensive data protection law.³¹

Only recently has internet diffusion become part of the Brazilian context. According to 'CETIC Domicílios' report, 51% (85.9 million) are internet users and within that statistics, 77% of them range from 16 to 24 years old.³² The current Brazilian legislation has already contemplated some aspects of internet access and uses.

The Brazilian Internet Bill of Rights (Art. 7)^{33,34}, also known as Marco Civil da Internet – approved by the National Congress in 2014, after a series of public consultations that started in 2009 – establishes that internet access is essential for exercising citizenship.³⁵ Further on, in 2011, the Access to Information Law (Law 12.527/2011) was sanctioned. Seeking to promote greater transparency in public administration, the law established mechanisms for mandatory disclosure of open data/files, especially in the internet, as well as any citizen's request for information online. Following from this public policy perspective, in 2010, the Ministry of Communications launched a National Plan for Broadband ('Plano Nacional de Banda Larga').³⁶ The plan sets quantitative goals and guidelines in order to stimulate the expansion of internet access in Brazil over the coming years.

It appears that not only Brazilian citizens³⁷, but also the government, understand the economic and social potential of the connected public sphere in Brazil and how it is playing an important role in the digital age in terms of access to knowledge, access to information, freedom of expression and accountability.³⁸

However, pointing towards another direction, a new context emerges rapidly and surreptitiously. Even though internet-related regulations such as the Marco Civil da Internet try to uphold the value and potential of the internet as well as stipulate practices that seek to protect constitutional rights, the current auto regulation based on code design³⁹ has proven to be able to overlap the rule of law reflected in these regulations. This auto regulation can subvert the traditional legal logic of 'ought to' that safeguards

citizens' free will, establishing a binary logic of 'can/can't', therefore leaving no alternative to citizens or governments' actions.⁴⁰

Harvard professor Lawrence Lessig called attention to the fact that the very architecture of the internet, that is, the hardware and software that make it up with technical structure and codes governing its functioning, are also ways to regulate human behaviour. According to Professor Lessig, regulation through architecture is sometimes even more effective than other more familiar forms such as law, economics (market) and social norms. That is why he coined the well known phrase "code is law"⁴¹, since the very architecture of the sites makes us hostage of the algorithms⁴², regulating our behaviour as well as the law and creating serious obstacles to access to information, individual autonomy, privacy and freedom of expression.⁴³

The internet is plastic and changeable and the fact that we are unwittingly becoming hostages of the algorithms that insert us on these bubbles, seeking the promise of hyperconnectivity and its facilities, has been seen as one of the most drastic changes, and subtle, because it is often unnoticeable.⁴⁴ In a techno-regulated context ruled by algorithms' binary logic of 'can/can't', the democratic potential of the connected public sphere and even the influence of the rule of law can be dramatically reduced.

The concept of rule of law is not easy to tackle. Tom Bingham brings a huge effort to describe the evolution of the concept and its meaning nowadays. According to Bingham⁴⁵, although we have an abstract idea of what it means as a 'law-governed state' and 'the laws of the land' and its importance for contemporary societies, it is hard to achieve a consensus about a closed concept.

Nevertheless, for the purposes of this article, we draw on Bingham's position, considering rule of law as the foundation of a civilised society that embodies a series of important interrelated ideas, as follows: first, it is responsible for limiting the power of the state. A government exercises its authority through publicly disclosed laws that are adopted and enforced by an independent judiciary in accordance with established and accepted procedures. Secondly, no one is above the law; there is equality before the law. Thirdly, there must be protection of the rights of the individual. Finally, the law must apply equally to the government and individual citizens.⁴⁶

Although Bingham considers the concept an ideal, the author agrees that it is an ideal worth striving for and envisions the connection of the rule of law with the concretion of fundamental and human rights. In that sense, we have a discrepancy between the role that the rule of law should represent in contemporary societies and the frequent disregard by private companies such as Facebook and YouTube through techno-regulation on the conduction of their platforms.⁴⁷

In 2004, UN Secretary-General Kofi Annan provided an expansive definition of the rule of law as:

"A principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency."⁴⁸

Algorithmic regulation of devices and platforms restricts the user to what has already been programmed. Furthermore, when it comes to algorithms and content providers,

content filtering and withdrawal are commonly automatised, rather invisible, and can even execute illegal (and demotivated) censorship without being held accountable to the user. Even though these kind of practices occur daily, private tech companies do not suffer any penalty. It is the techno-regulation overlapping the rule of law.

According to Ugo Pagallo,

“Where non-normative instruments dominate the regulatory environment, we seem to be subject to the rule of technology rather than the rule of law. It may be time to realise the fact that increase in efficiency do not always result with effective solutions. ‘To prevent becoming merely the cognitive resource for these environments we must figure out how they are anticipating us.’ In a techno-regulatory setting, rules no longer embody the politics that they are based on, but they simply dictate it. Law and politics do not operate as two exclusive axioms namely, ‘politics is the field of power relations and contestations; and law is the sphere of truth and justice governed by the rule of law.’ Techno-regulation signals the demise of our capacity to reason against and resist, and thus it may result with a further deviation from the values that make us ‘human’.”⁴⁹

To illustrate this problem connecting to an IoT context, recently, Samsung warned its customers not to discuss personal information in front of Samsung’s smart TV’s. The news came after a declaration pointing out a disturbing line in the privacy policy of Samsung: “Please be aware that if your spoken words coming from your TV include personal or confidential information, this information will be among the data captured and transmitted to third parties.”⁵⁰ This case raises the issue that although some of the threats and risks of the IoT scenario does not seem novel, many of the threats and challenges are seriously amplified in this context considering the new processes of storage, treatment and sharing of the massive amount of personal data being generated.

Other examples, Youtube’s blocking mechanism of techno-regulation through content ID system⁵¹ severely jeopardises the Brazilian remix culture coming from Funk⁵² and Tecnobrega⁵³ expressions in the music scene. Meanwhile, Facebook’s algorithm, trying to filter pornography expressions, recently censored a post by the Ministry of Culture in Brazil (posted in its official Facebook profile) with a photograph picturing two Brazilian natives. The photo in the public domain was posted as a release to divulge a new website in partnership with the National Library Foundation and the Moreira Salles Institute containing in the collection over two thousand historical images of the nineteenth and twentieth centuries. Given the lack of transparency for the automatic filtering and the indifference demonstrated by the Facebook in this case, Brazilian Minister of Culture publicly declared that the algorithm’s private censorship was abusive, violating the rights to freedom of expression, sovereignty and access to culture, further demanding explanations by the company and threatening them with a possible judicial prosecution.⁵⁴

All those examples give us a clear perspective that techno-regulation is already an established practice, that is being articulated to address specific commercial purposes without observing constitutional rights or specific internet regulations such as those foreseen in recently approved Internet Bill of Rights (Marco Civil da Internet), document that emphatically states the importance of guaranteeing constitutional rights in cyberspace.

It is important to assert that it must not be the intent of the law to govern this process in a way that hinders the advance of technology. Differently, we must be conscious that if techno-regulation by code is growing faster than our ability to guarantee safety and

privacy for users and we are already failing on having an adequate regulatory framework upheld by the law, an adequate legal framework is necessary to respond to those new legal challenges. Moreover, a deep reflection is necessary about to what extent the normative side of the law should be transferred from the traditional 'ought to' of legal systems to automatic techniques through mechanisms of design, codes, and architectures.⁵⁵

The lack of specific regulation, in Brazil for instance, safeguarding personal data, makes it an even worse scenario, facilitating companies to close deals based on online information produced by its clients (users) using their services. This feeds the economic force of private companies, further simulating unclear and unfair relationship that involve practices that are challenging to track – treating data that, most of the times, is beyond the scope of their services and products.

To illustrate, recently research from the Centre for Technology and Society at FGV Direito Rio for the Dynamic Coalition on Platform Responsibility working group of the Internet Governance Forum showed that more than 66% of the analysed internet platforms gathered more data than what would be necessary for the accomplishment of the service contracted by the user.⁵⁶

In Brazil, Facebook and SERASA (company created by the banks so they would, among other purposes, be able to analyse and research the economic/financial information of their clients for services such as credit loans) made public their interest in closing a partnership that would allow the social network company to access the financial company's data banks. With that, companies would be able to direct ads to a specific audience according to their income based on the information provided by Facebook. This invasive practice may change the way that we view ad-based publicity contracts promoted by Facebook and its partners.⁵⁷

Additionally, there is a rising number of start-ups using users' information taken from social media to develop an index capable of determining the reliability of a potential borrower. With that in mind, companies would have greater security in loaning services, knowing who can/can not honour their debts. Based on such information, they could also offer lower tax rates to those that were better evaluated.⁵⁸ Social groups, especially the economical vulnerable ones, have been suffering from discriminatory practices, namely, the massive use of online personal data crossing.

Another practice worth mentioning is 'digital redlining'. The term redlining refers to the imaginary red line drawn by banks in poor neighbourhoods to mark people within a geographic location and to whom higher taxes are destined. This exclusion and discrimination was now imported into the digital world, elaborated not by a map anymore, but by a robot that integrates imported data (among others) from social networks. They gather most of these data from networks such as Facebook, so that they may establish higher tax rates for certain people.

Even though public policy makers and citizens in Brazil appear to be more conscious of the internet's economic and social potential, they are not sufficiently aware of the risks that may arise from private companies' practices or the enhanced risks to fundamental rights imposed by big and open data and the enlargement of the IoT environment.

Besides the urgent necessity of developing a specific legislation about personal data and privacy protection to avoid unconstitutional techno-regulation or personal data treatment, we should seek more broadly an efficient regulation of these technologies through a meta-technological perspective of the law.

The legal order and the rule of law, differently from other social orders, regulates human behaviour by means of a specific technique. Once such technique regulates other techniques that orient behaviours and, beyond that, processes of technological innovation, we may accordingly conceive the law as a meta-technology.

According to Ugo Pagallo⁵⁹,

“The different and even opposite ways in which we can grasp the normative purposes of the law as a meta-technology recommend to expand our view. We propose four steps of analysis. First, a meta-regulatory approach to the field of legal automation should allow us to determine whether, and to what extent, lawmakers shall not (or cannot) delegate decisions to automated systems. Second, focus should be on the impact of technology on the formalisms of the law, and how the latter competes with further regulatory systems. Third, we have to pay attention to the principles and values which are at stake with the delegation of decisions to automated systems, namely the institutional dimension of the law with matters of interpretation and deliberation. Fourth, the distinction between automatic and non-automatic decisions of the law, and their legitimacy, may entail a class of legal problems, i.e., the hard cases of the law (...).”

Bearing in mind the importance of the law as an effective system for regulating behaviour and actions, as well as considering that its criterions also take into account the need to guarantee constitutional rights while concomitantly preserving human autonomy, the rule of law has to guide technology and not the opposite. As Lawrence Lessig once stated, the threat is that “controls over access to content will not be controls that are ratified by courts; the controls over access to content will be controls that are coded by programmers.”⁶⁰

Therefore, before the enhanced risks imposed by the advancement techno-regulation, amplified by the spread of the IoT environment, the rule of law must be seen as the premise for developing technology, or as a meta-technology, that should guide behavioural technological regulation and not the contrary – often resulting in the violation of rights.

Stefano Rodotà highlights the importance of the law as a regulatory instrument in a context of growing technology considering that if we do not consider the internet as a ‘constitutional’ space, rich in adequate guarantees, security and control may prevail, as it is threatening to happen in this period. All in all, the logic of the market, that is already imposing rules, would succeed because most of online activities are somehow commercial and the Web is considered to be a great mine of personal data. The persistent need to consider these problems as ‘constitutional’ clearly indicates what paths the law must take if one needs adequate responses to the new shapes technologies are giving to societies.⁶¹

4 Conclusions

The IoT becomes more prominent every day. Developed in the context of evolution of digital technologies and being considered by many as a new paradigm (Web 3.0), this new context represents a new and exciting time for both companies and consumers.

In principle, the idea of having interconnected smart devices enabling efficient interaction between machines and humans, helping those in their daily tasks, may seem a

uniquely beneficial scenario. Furthermore, if considered individually, the information generated by the devices and online platforms may seem irrelevant and even harmless.

However, when combined, these data can reveal a detailed and individualised consumer profile. This possibility has increasingly attracted the interest of companies seeking through information crossing techniques, get an unprecedented view of their consumers.⁶²

The data from these various interconnected devices, generated spontaneously and deliberately by users, may pose risks to constitutional rights of users such as privacy and security, exposing them to enhanced risks and losses that they are not yet fully aware.

Adding up to the increased potential for damage and challenges posed by the context of IoT, there is still no satisfactory regulation by the law on personal data protection in Brazil. It is an urgent necessity. Despite being civilly and constitutionally protected values, it is necessary for a specific law to ensure the enforcement of the security and privacy of users in this techno-regulated scenario from a meta-technology perspective of the law.

The rule of law has an important role to play in the consolidation of constitutional rights in the connected public sphere. Without legal and binding obligations to review private companies' practices such as unconstitutional algorithmic filtering, uninformed content removal or treatment and sharing of personal data beyond the object of a certain service, these practices tend to increase even more with the enlargement of the IoT. The challenge is to observe and analyse these practices and measure their importance and risks while seeking to guide technology through efficient legal regulation, preserving autonomy, privacy, freedom of expression and users' safety.

In the words of Paul Ohm: "Regulators must respond rapidly and forcefully to this disruptive technological shift, to restore balance to the law and protect all of us from imminent, significant harm."⁶³

On the other hand, the users voluntarily provide their data online, feeding databases with a huge amount of personal information, without worrying about how operators oversee and treat their information. Therefore, it is essential that consumers be well aware of these risks and be even more careful with their data in an IoT environment.

No one knows for sure how the IoT will affect our lives in the future. Integrated, related, targeted and combined data collected from smart devices, providing numerous opportunities for analysis of this information and converting each information in a relevant information to be combined and analysed. Whether or not, the way we interact with machines and algorithms tends to be more and more intense. In this context IoT, governance and data security will be key. Businesses and consumers should weigh benefits and risks cautiously. Moreover, the law should be aware of its role in this context aiming to, on one side, not excessively hamper the economic and technological development in progress, and, on the other, regulate effectively these practices in order to curb abuses and protect the existing constitutional rights.

Notes

- 1 Nike Running (2012) *The New Nike+Running App*, YouTube, 26 June [online] <https://www.youtube.com/watch?v=HF-bV1Lar1k> (accessed 16 March 2016).
- 2 *Computer Science Zone Security and the Internet of Thing* [online] <http://www.computersciencezone.org/wp-content/uploads/2015/04/Security-and-the-Internet-of-Things.jpg#sthash.c6u2POMr.dpuf> (accessed 11 February 2017).

- 3 Federal Trade Commission (2015) *Internet of Things: Privacy & Security in a Connected World*, Federal Trade Commission, Washington.
- 4 NIC.br (2014) *A Internet das coisas, explicada pelo NIC.br*, YouTube, 16 July [online] [online] <https://www.youtube.com/watch?v=jlkvzcG1UMk> (accessed 16 March 2016).
- 5 Federal Trade Commission (2015) *Supra Note 3* [online] <https://pt.scribd.com/doc/253953070/FTC-IofT-Staff-Report-pdf> (accessed 14 November 2017).
- 6 Barker, C. (n.d.) *25 Billion Connected Devices by 2020 to Build the Internet of Things*, ZDNet [online] <http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/> (accessed 23 February 2017).
- 7 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. (2000) 'Code is law: on liberty in cyberspace', *Harvard Magazine*, pp.1–2 [online] <https://harvardmagazine.com/2000/01/code-is-law-html> (accessed 28 March 2017).
- 8 Techno-regulation is the intentional influencing of human behaviour through the implementation of values, norms and rules in technological devices.
- 9 Santucci, G. (2010) 'The internet of things: between the revolution of the internet and the metamorphosis of objects', *Vision and Challenges for Realising the Internet of Things*, pp.11–24 [online] <http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-internet-revolution.pdf> (accessed 12 February 2017).
- 10 ITU (n.d.) *Internet of Things Global Standards Initiative*, ITU Committed to Connecting the World [online] <http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx> (accessed 12 February 2017).
- 11 Pontin, J. (2005) 'ETC: Bill Joy's six webs', *MIT Technology Review* [online] <https://www.technologyreview.com/s/404694/etc-bill-joys-six-webs/> (accessed 12 February 2017).
- 12 Hapgood, F. (2007) *20 Years of IT History: Connecting Devices, Data and People*, CIO, 28 September [online] <http://www.cio.com/article/2438016/infrastructure/20-years-of-it-history--connecting-devices--data-and-people.html> (accessed 12 February 2017).
- 13 Ashton, K. (2009) 'That 'internet of things' thing', *RFID Journal*, 22 June [online] <http://www.rfidjournal.com/articles/view?4986> (accessed 12 February 2017).
- 14 Big Thing (2012) *Web 3.0*, YouTube, 23 April [online] (accessed 16 March 2016).
- 15 O'Reilly Net (2004) *Web 2.0 Conference* [online] <http://conferences.oreillynet.com/web2con/> (accessed 12 February 2017).
- 16 Aghaei, S. (2012) 'Evolution of the World Wide Web: from Web 1.0 to Web 4.0', *International Journal of Web & Semantic Technology*, Vol. 3, No. 1, pp.1–10.
- 17 Ray, K. (2010) *Web 3.0*, Vimeo, 6 May [online] (accessed 16 March 2016).
- 18 Markoff, J. (2006) 'Entrepreneurs see a web guided by common sense', *The New York Times*, 12 November [online] <http://www.nytimes.com/2006/11/12/business/12web.html> (accessed 12 February 2017).
- 19 Aghaei, S., Nematbakhsh, M.A. and Farsani, H.K. (2012) 'Evolution of the World Wide Web: from Web 1.0 to Web 4.0', *International Journal of Web & Semantic Technology*, Vol. 3, No. 1, pp.1–10.
- 20 Ibid.
- 21 Shannon, V. (2006) 'A 'more revolutionary' web', *The New York Times*, 23 May [online] <http://www.nytimes.com/2006/05/23/technology/23iht-web.html> (accessed 12 February 2017).
- 22 Berners-Lee, T., Hendler, J. and Lassila, O. (2001) 'The semantic web', *Scientific American*, Vol. 284, No. 5, pp.28–37.

- 23 Shadbolt, N., Berners-Lee, T. and Hall, W. (2006) 'The semantic web revisited', *IEEE Intelligent Systems*, Vol. 21, No. 3, pp.96–101.
- 24 Bajarin, T. (2014) 'The next big thing for tech: the internet of everything', *Time*, 13 January [online] <http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/> (accessed 12 February 2017).
- 25 Weissberger, A. (2014) *Are the Internet Of Things (IoT) & Internet Of Everything (IoE) the same thing?*, The Viodi View, 24 May [online] <http://viodi.com/2014/05/23/are-the-internet-of-things-iot-internet-of-everything-iot-the-same-thing/> (accessed 12 February 2017).
- 26 Patel, K. (2013) 'Incremental journey for World Wide Web: introduced with Web 1.0 to recent Web 5.0 – a survey paper', *International Journal of Advanced Research in Computer Science and Software Engineering*, October, Vol. 3, No. 10, pp.410–417.
- 27 Castells, M. (1999) *A Sociedade em Rede – A Era da Informação: Economia, Sociedade e Cultura*, Vol. 1, Paz e Terra, São Paulo.
- 28 Benkler, Y. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale University Press, New Haven London.
- 29 With some differences, varying according to their own conceptions of what would be the Internet and its focus of research, the so-called cyber-skeptics share common concerns. Andrew Keen, Nick Carr, Cass Sunstein, Richard Wurman, Mark Bauerlein, Steve Talbot, Jaron Lanier, Matthew Hindman, Sherry Turkle, Evgeny Morozov, Eli Pariser e Tim Wu are names that, at some point, have been or are associated with this current, each with its own vision, with skeptical doses for specific aspects or reticent about the democratic potential of the internet. Eli Pariser analyses the democratic loss generated by the invisible filter that puts us in a bubble where everything pleases, everything makes sense and everything is in line with our visions and realities. These mechanisms, increasingly sophisticated, impressive in showing, most of the time, agreeable information, depriving us of dissonant voices. Pariser, E. (2011) *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Press, New York.
- 30 Almeida, V.A.F., Doneda, D. and Monteiro, M. (2015) 'Governance challenges for the internet of things', *IEEE Internet Computing*, Vol. 19, No. 4, pp.56–59.
- 31 Pagallo, U. (2013) *The Laws of Robots: Crimes, Contracts, and Torts*, Springer, Torino.
- 32 Brazilian Network Information Center survey on the use of ICT in Brazil: ICT households and enterprises 2013. CETIC.br (2014) *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação no Brasil – TIC Domicílios e Empresas 2013*, Cetic.br – Centro Regional Para O Desenvolvimento Da Sociedade Da Informação [online] http://cetic.br/media/docs/publicacoes/2/TIC_DOM_EMP_2013_livro_eletronico.pdf (accessed 12 February 2017).
- 33 Brasil (2014) *Marco Civil da Internet*, Act no. 12.965/2014 [online] http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm (accessed 12 February 2017).
- 34 Edward Snowden cites the Marco Civil da Internet. Snowden, E. (2015) *A sociedade aberta avança*, El País, 4 June [online] http://brasil.elpais.com/brasil/2015/06/04/opinion/1433436340_438817.html (accessed 12 February 2017).
- 35 The project bill of 'Marco Civil da Internet' was set in a context in which Brazilian representatives, academics and civil society organisations have worked together to bring more legitimacy and participation in the process of creating laws through the use of internet platforms. The draft represented a commendable state initiative to expand the debate and communication skills in the preparation of rules. The online public consultation promoted by the government, incremented the debate in the public sphere opening channels for discussing the content and procedures of the rules aiming a greater acceptance of the law. However it is important also to see beyond the process' merits. This deliberative process, despite being commendable and novel in Brazil, also experienced limitations to its potential, for instance, not all expressions were contemplated due to challenges such as lack of Internet access, the effects of technicalisation of debate and the strong lobby imposed by some private sectors. Nevertheless, considering that it was the first experience of legislative online consultation in Brazil, it has already been a good advancement. But it is important that in the next similar processes both civil society and government try to correct these flaws and make viable all

- possible resources for digital inclusion and capacitate citizens for the debate, expanding the capacity to absorb the expression of all possible affected by the rule.
- 36 Ministério das Comunicações (n.d.) *Plano Nacional de Banda Larga* [online] <http://www.mc.gov.br/programa-nacional-de-banda-larga-pnbl> (accessed 8 November 2016).
 - 37 The American National Congress recently created a specific commission to discuss issues concerning IoT. Kravets, D. (2015) 'Internet of things: there's now a US congressional committee for that', *Ars Technica*, 13 January [online] <https://arstechnica.com/tech-policy/2015/01/internet-of-things-theres-now-a-us-congressional-committee-for-that/> (accessed 12 February 2017).
 - 38 Faria, C.F.S.D. (2012) *O parlamento aberto na era da internet: pode o povo colaborar com o Legislativo na elaboração da leis?*, Câmara dos Deputados, Edições Câmara [online] <http://bd.camara.gov.br/bd/handle/bdcamara/7867> (accessed 12 February 2017).
 - 39 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" See Lessig, L. (2000) *supra* note 7.
 - 40 Pagallo, U. (2015) 'Good online governance: on law, spontaneous orders, and design', in Floridi, L. (Ed.): *The Online Manifesto: Being Human in a Hyperconnected Era*, Springer, London.
 - 41 Lessig, L. (2000) *supra* note 7.
 - 42 The critics to algorithmic architecture in this paper can also be expanded to hardware architecture.
 - 43 Lessig, L. (2006) *Code*, Version 2.0, Basic Books, New York.
 - 44 Former president of the USA, Barack Obama recently shed light on the filter bubble effect as a democratic issue on his farewell speech: Fuller, Z. (2017) *Obama's Farewell Speech Frames Filter Bubbles as a Personal Responsibility*, MIDiA Research, 11 January [online] <https://www.midiaresearch.com/blog/obamas-farewell-speech-frames-filter-bubbles-as-a-personal-responsibility/> (accessed 12 February 2017).
 - 45 Bingham, T.H. (2001) *The Rule of Law*, Penguin, London.
 - 46 *Ibid.*
 - 47 *Ibid.*
 - 48 United Nations Security Council (2004) *Report of the Secretary-General S/2004/616* [online] www.un.org/en/ga/search/view_doc.asp?symbol=S/2004/616 (accessed 12 January 2017).
 - 49 Pagallo (2015) *supra* note 40.
 - 50 Democratize (2016) *Samsung alerta clientes para não discutir informações pessoais na frente de smart TV's*, Medium, 12 February [online] <https://medium.com/democratize-m%C3%ADdia/samsung-alerta-clientes-para-n%C3%A3o-discutir-informa%C3%A7%C3%B5es-pessoais-na-frente-de-smart-tv-s-88a42230a0d#rfeb6cpkn> (accessed 12 February 2017).
 - 51 Youtube (n.d.) *Como funciona o Content ID* [online] <https://support.google.com/youtube/answer/2797370?hl=pt-BR> (accessed 22 February 2016).
 - 52 Wikipedia, The Free Encyclopedia (2017) *Funk Carioca*, 12 February [online] https://en.wikipedia.org/wiki/Funk_carioca (accessed 22 February 2016).
 - 53 Wikipedia, The Free Encyclopedia (2016) *Tecno Brega*, 19 February [online] https://en.wikipedia.org/wiki/Tecno_brega (accessed 24 February 2016).
 - 54 Ministério da Cultura (2015) *Ministério da Cultura – Ministro Juca Ferreira concede entrevista coletiva sobre medidas legais contra Facebook – Notícias Destaques*, MinC [online] http://www.cultura.gov.br/noticias-destaques/-/asset_publisher/OiKX3xIR9iTn/content/id/1248553 (accessed 12 February 2017).
 - 55 Pagallo, U. (2012) 'Cracking down on autonomy: three challenges to design in IT law', *Ethics and Information Technology*, Vol. 14, No. 4, pp.319–328.

- 56 *Recommendations on Terms of Service and Human Rights* for the Dynamic Coalition on Platform Responsibility working group of the Internet Governance Forum (Report to be divulged in 2016).
- 57 Junior, H. (2015) *Facebook e Serasa fecham parceria para anúncios segmentados por renda*, 10 June [online] <https://www.linkedin.com/pulse/facebook-e-serasa-fecham-parceria-para-anuncios-por-renda-junior> (accessed 12 February 2017).
- 58 Evangelista, R. (2015) *Na era da Discriminação Digital*, Outras Palavras, 3 June [online] <http://webcache.googleusercontent.com/search?q=cache:ZQVUYW4GZjYJ:outraspalavras.net/posts/na-era-da-discriminacao-digital/+&cd=1&hl=pt-BR&ct=clnk&gl=br> (accessed 12 February 2017).
- 59 Pagallo, U. and Durante, M. (2016) 'The pros and cons of legal automation and its governance', *European Journal of Risk Regulation*, Vol. 7, No. 2, pp.323–334.
- 60 Lessig, L. (2004) *Free Culture: The Nature and Future of Creativity*, Penguin Press, New York, NY.
- 61 Rodotà, S. (2003) *Palestra no Rio de Janeiro* [online] <http://www.rio.rj.gov.br/dlstatic/10112/151613/DLFE-4314.pdf/GlobalizacaoDireito.pdf> (accessed 12 January 2017).
- 62 Baptista, R. (2015) *Porque a Internet das Coisas implica em gerenciar contextos, e não dados*, TI Rio SeproRJ, 2 July [online] <http://www.tirio.org.br/info/36007/porque-a-internet-das-coisas-implica-em-gerenciar-contextos-e-nao-dados> (accessed 12 February 2017).
- 63 Ohm, P. (2010) 'Broken promises of privacy: responding to the surprising failure of anonymization', *UCLA Law Review*, Vol. 57, p.1701.