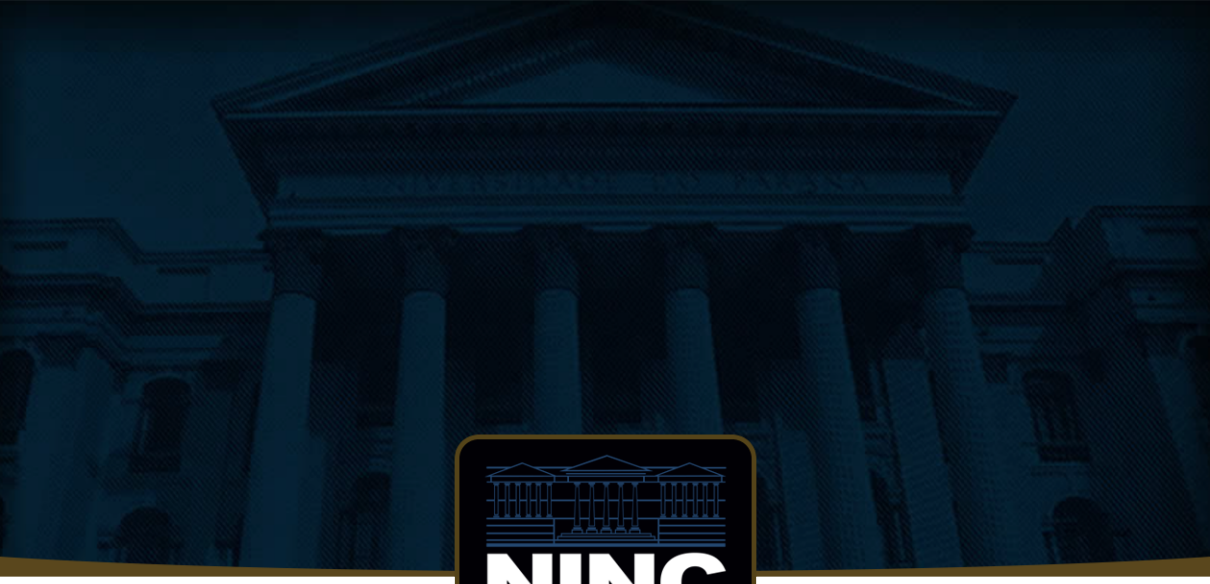

NINC
NÚCLEO DE INVESTIGAÇÕES CONSTITUCIONAIS
UFPR

REVISTA DE INVESTIGAÇÕES CONSTITUCIONAIS

JOURNAL OF CONSTITUTIONAL RESEARCH

vol. 6 | n. 2 | maio/agosto 2019 | ISSN 2359-5639 | Periodicidade quadrimestral
Curitiba | Núcleo de Investigações Constitucionais da UFPR | www.ninc.com.br

Revista de Investigações Constitucionais
ISSN 2359-5639
DOI: DOI: 10.5380/rinc.v6i2.67592

The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy

A aplicabilidade da Internet das Coisas (IoT) entre os direitos fundamentais à saúde e à privacidade

MATEUS DE OLIVEIRA FORNASIER [I, *]

[I] Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Brasil)
mateus.fornasier@unijui.edu.br
https://orcid.org/0000-0002-1617-4270

Recebido/Received: 25.06.2019 / June 25th, 2019
Aprovado/Approved: 25.11.2019 / November 25th, 2019

Abstract

This work aims to study main insecurities and uncertainties regarding to IoT, verifying its impact to the exercise of the fundamental rights to healthcare and to privacy. Its specific objectives are: i) to present promises of IoT to healthcare and treatments; ii) to expose risks and uncertainties identified with IoT until the present moment; iii) to analyze ethical and legal principles (mainly in Brazil) concerning to IoT uses. Its main hypothesis is that healthcare can be revolutionarily improved with IoT, but despite of all of that revolution in good practices, good technologies of security, securitized by public policies and legal practices, have also to be implemented and improved by scholars, jurists and politicians. Methodology: hypothetical-deductive method of research, with a qualitative and transdisciplinar method of approach, and a bibliographical research technique. Results: IoT/IoMT presents a great potential of actualization of the fundamental right to health, but the security of the collection and storage of sensitive data should be the first concern

Resumo

este artigo visa estudar as principais inseguranças e incertezas concernentes à IoT, verificando seu impacto ao exercício dos direitos fundamentais à saude e à privacidade. Seus objetivos específicos são: i) apresentar promessas da IoT aos serviços e tratamentos de saúde; ii) expor riscos e incertezas identificados com a IoT até o momento presente; iii) analisar princípios éticos e jurídicos (principalmente do Brasil) relacionados aos usos da IoT. Sua hipótese principal é de que os serviços de saúde podem ser revolucionariamente melhorados com a IoT, mas apesar de toda essa revolução em boas práticas, boas tecnologias de segurança, asseguradas por políticas públicas e práticas legais, também têm de ser implementadas e aperfeiçoadas por teóricos, juristas e políticos. Metodologia: método de pesquisa hipotético-dedutivo, com um método de abordagem qualitativo e transdisciplinar, e técnica de pesquisa bibliográfica. Resultados: IoT/IoMT apresenta um grande potencial de efetivação do direito fundamental à saúde, mas a segurança da coleta e armazenamento de dados sensíveis deve ser a primeira

Como citar esse artigo/*How to cite this article*: FORNASIER, Mateus de Oliveira. The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy. **Revista de Investigações Constitucionais,** Curitiba, vol. 6, n. 2, p. 297-321, maio/ago. 2019. DOI: 10.5380/rinc.v6i2.67592.

[*] Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (Unijuí-RS Brasil). Doutor em Direito pela Universidade do Vale do Rio dos Sinos (Unisinos, Brasil), com Pós-Doutorado pela University of Westminster (Reino Unido). E-mail: mateus.fornasier@unijui.edu.br.

in the development of systems involving such technologies, since there is an immense potential of disrespect to the fundamental right to the privacy of individuals from their use, not only by private third parties, but also, by the State.

preocupação no desenvolvimento de sistemas envolvendo tais tecnologias, pois há um imenso potencial de desrespeito ao direito fundamental à privacidade dos indivíduos a partir do seu uso, não apenas por terceiros privados, mas também, por parte do Estado.

Keywords: Internet of Things; healthcare; sensible data; security; privacy.

Palavras-chave: *Internet das Coisas; serviços de saúde; dados sensíveis; segurança; privacidade.*

CONTENTS

1. INTRODUCTION

The first Industrial Revolution (IR) started in Britain around late 18th century with steam and water power transferring manual labor from homes to powered textile machines in factories. The second one came in the early 20th century, with internal combustion engines and electrical power generation (allowing mass production of automobiles, for example). The third IR took place in 1990s with electronics, personal computers, and IT being in the automated production systems. Along with technological advancements and life quality improvements, such revolutions polluted air and water pollution and warmed the planet.

In recent years, it has been communicated that the Internet of Things (IoTs) and data analytics are the most significant emerging technologies that have a transformational and disruptive effect to global industry. By digitizing the physical world, IoT can be a driver to the fourth IR. Its application to our lives opens up new opportunities and challenges for governments, enterprises, and individuals.[1]

Coined by Kevin Ashton in his presentation made to Procter & Gamble (P&G) in 1999,[2] the term "Internet of Things" describes a system consisting of network sensors, actuators, and smart objects whose purpose is to interconnect 'all' things, including everyday and industrial objects, in such a way that turns them intelligent, programmable, and more capable of interacting with humans and other devices.[3] The internet of things

---

1 GENG, Hwaiyu. Internet of Things and Data Analytics in the Cloud with Innovation and Sustainability In: GENG, Hwaiyu. **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 21- 79; p. 24-25.

2 GENG, Hwaiyu. Internet of Things and Data Analytics in the Cloud with Innovation and Sustainability In: GENG, Hwaiyu. **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 21-79; p. 28.

3 IEEE Standards Association (IEEE-SA). **Internet of Things (IoT) Ecosystem Study.** IEEE Standards Association, The Institute of Electrical and Electronic Engineers, Inc., 2015. Disponível em: https://iot.ieee.org/images/files/pdf/iot_ecosystem_exec_summary.pdf.Acesso em: 4 fev 2019, p. 1.

(IoT) is a technology that enables identifiable computing devices embedded with other interfaces (i.e. humans and machines) linked via networks (wired or not) in order to catch data from the environment it has been exposed, creating an information network to provide digital business models and new services and functionalities.[4] Some have said that, with the advancement in computing, from the decade of 2010s on we are gradually configuring an era of the IoT - and this technology is gaining world popularity as it captures data from the environment through sensors (which are becoming cheaper and more powerful each day, as it happens with other computing devices).[5] The reduction of the cost of computing power, as well as the implementation of new technologies (such as the IPV6, which allows connecting almost everything on Earth) prospect the growth of IoT, and an enormous opportunity to connect bot new and existing services in business, education, utilities and healthcare - creating smart-living offerings in the cities with real-time efficiency.[6]

The greatest examples of the potential of the IoT that can be designed and implemented for human benefit go from connected cars to smart cities, passing through smart retail, smart traffic systems and smart factories:[7] smart cities can have IoT-enabled services (i.e. water management and distribution, energy generation and transmission, logistics, garbage disposal and management, street-lightening, healthcare, surveillance and security, e-governance, etc.); connected cars could permit establishing systems to monitor fuel levels, location, crash prevention, travel-route optimization (with real-time traffic analysis and driverless communication); smart traffic systems could be enabled with IoT in a traffic network of a city to determine the flow of traffic in order to permit necessary decisions to avoid traffic jam and chaos; factories could be more energy efficient with its monitoring, as well as their machines and components could be better treated and replaced by technicians; sensor-based and data-based monitoring of consumer behavior in retail outlets can help the owners to understand specific behavior and product choices, carting facilities to track the items selected by consumers for automated payment and billing through smart phones can alter the business' models; current smart watches help monitor and report physical activities of humans and critical health parameters (i.e. blood pressure, heart rate, etc.) - which can be enhanced to the point of permitting digital health service revolution (also permitting

4 CHAUDHURI, Abhik. **Internet of things, for Things, and by Things**. Boca Raton: CRC Press, Taylor & Francis Group, 2018, p. 50.

5 CHAUDHURI, Abhik. **Internet of things, for Things, and by Things**. Boca Raton: CRC Press, Taylor & Francis Group, 2018, p. 52.

6 CHAUDHURI, Abhik. **Internet of things, for Things, and by Things**. Boca Raton: CRC Press, Taylor & Francis Group, 2018, p. 58.

7 CHAUDHURI, Abhik. **Internet of things, for Things, and by Things**. Boca Raton: CRC Press, Taylor & Francis Group, 2018, p. 60-63.

other wearable and implanted devices be monitored by physicians in order to make decisions and prescript drugs).[8]

Along with robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, 3D printing and autonomous vehicles, the "Internet of Things" mark the fourth industrial revolution. Particularly, it is a concept with potential to impact human lives, improving dramatically security, energy efficiency, education, health, and many other aspects of daily life. It also improves decision-making and productivity of enterprises.[9]

This article is limited to the analysis of IoT issues to fundamental rights (mainly privacy) when such technology is applied to healthcare. Not only matters related to technology itself, but also to juridical and legal questions will be approached in order to develop an initial theoretical landmark for discussing Constitutional Law along such technology development.

The main goal of this work, then, is to study the main insecurities and uncertainties regarding to IoT, verifying its impact to the exercise of the fundamental rights to healthcare and to privacy. In order to do so, the text was divided into three parts. The first one will present promises of IoT to healthcare and treatments as IoT is being implemented to such fields. The second one is destined to expose risks and uncertainties identified until the present moment, as media and science are communicating about them. The third one aims to analyze ethical and legal principles (mainly in Brazil) concerning to IoT uses.

The research problem that drove this work can be described this way: as IoT is getting inside everyday life in several devices, including healthcare, which are the main concerns regarding to security legal systems have to develop in order to evolute in a manner that can make the fundamental right to health become more efficient without being too permissive about the right to privacy?

The primal hypothesis to such questioning is that healthcare can be revolutionarily improved with such technology, making health monitoring a wireless and

---

[8] The IoT's potential can be utilized to realize the Sustainable Development Goals (SDGs) of the United Nations' "2030 Agenda for Sustainable Development". Paragraph 15 of the Agenda, which aims to transform our world, specifically mentions and acknowledges the potential of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies as does scientific and technological innovation across areas as diverse as medicine and energy. In the other hand, the report "Harnessing the Internet of Things for Global Development", written as a contribution to the ITU/UNESCO Broadband Commission for Sustainable Development, provides multiple examples of IoT interventions that have been mapped to the Millennium Development Goals (MDGs) and Sustainable Development Goals (SDGs) in various sectors like health, water and sanitation; agriculture and livelihoods; education; the environment and conservation; resiliency, infrastructure and energy; governance and human rights.

[9] SHARMA, Neha; SHAMKUWAR, Madhavi; SINGH, Indjerit. The History, Present and Future with IoT In: BALAS, Valentina et al. (ed.). **Internet of Things and Big Data Analysis for Smart Generation**. Cham: Springer, 2019, p. 101-160; p. 103.

omnipresent activity, dismissing lots of current inefficient practices (such as *in locus* consultations and batteries of examinations). But despite of all of that revolution (which can make the right to health much more concretized in practice, as it demands less professionals, for example) in good practices, good technologies of security, securitized by public policies and legal practices, have also to be implemented and improved by scholars, jurists and politicians.

About the methodology, the research method used for this paper is hypothetical-deductive, as it parts from a main hypothesis that is tested all along its development. Its method of approach is qualitative and transdisciplinar, because the main characteristics and basis of every argument are used, extracted from several fields of knowledge to analyze their potential transformations to the domain of Law. And its research technique is mainly bibliographical.

2. IOT ENHANCING THE FUNDAMENTAL RIGHT TO HEALTH: PROMISES FROM PRESENT TO THE FUTURE

IoT enables information flows from/to and among heterogeneous, highly distributed, real and virtual devices (smart devices, sensors, actuators, etc.). Although its concept originated to enable communication among various types of physical objects for the provision of smart applications, IoT has evolved to enable forms of collaboration and communication between people and things.[10] IoT, when applied to medical issues, plays a fundamental role in remote healthcare, in monitoring health devices to increase their efficient usage, and improving the speed and accessibility of health services.[11] It can be used to collect health data from patients through wearables connected to the internet, connecting and communicating in machine-to-machine (M2M) through communicating medical devices. Received data from such devices are stored in a cloud server database linked to platforms, and then, analyzed.

According to Sinnapolu and Alawneh,[12] Android and iOS based smartwatches already contain technology enough to measure blood pressure and heart rate - which, when added to cloud computing could make available for healthcare data enough to trace prognostics about chronic disease such as heart attack, high blood pressure and coronary disease. Healthcare for elderly people (over 65 years old), for exemple,

---

[10] MIHOVSKA, Albena; PRASAD, Ramjee; PEJANOVIC, Milica. **Human-centered IoT Networks** In DIXIT, Sudhir (ed.). **Human bond communication:** the holy grail of holistic communication and immersive experience. Hoboken: John Wiley & Sons, Inc., 2017, p. 178.0-219.0; p. 179.0.

[11] GUNTUR, Sitaramanjaneya Reddy; GORREPATI, Rajani Reddy; DIRISALA, Vijaya R. Internet of Medical Things: remote healthcare and Health Monitoring Perspective In: HASSANIEN, Aboul Ella; DEY, Nilanjan; BORRA, Surekha. **Medical Big Data and Internet of Medical Things:** advances, challenges and applications. Boca Raton: CRC Press, Taylor & Francis Group, 2019, p. 633-703; p. 637.

[12] SINNAPOLU, GiriBabu; ALAWNEH, Shadi. Integrating wearables with cloud-based communication for health monitoring and emergency assistance. **Internet of Things**, v. 1–2, 2018, p. 40–54.

is a very important issue, mainly concerning to chronic diseases - and that sector of population is increasing over the years; then, a rapid adaptation of smartphones and web applications makes them, together with wearables, a preferred platform for health monitoring.[13]

IoMT has potential to reduce days and admissions in healthcare institutions due to the mobility of the wearables, which allow 24/7 monitoring of patients. Patients can recover in the comfort of his/her own surroundings since personalized health care services are now possible anywhere and anytime the patient demands it. The patient would have, then, the opportunity to take care of herself/himself and play a more active role in the care process.[14]

But not only on wearables and smartphones can IoMT rely: other ideas for wider structures are being proposed. Milocanovic and Bojkovic[15] have listed several healthcare solutions related to IoMT: ambient assisted living (AAL) (extensions for independent life of elderly individuals in a safe manner, giving them human servant-like assistance in case of any problem); internet of m-health things (m-IoT) (internet-based mobile computing, medical sensors and communication technologies for healthcare services); adverse drug reaction (the patient's device identifies the drug by means of barcode); community healthcare (CH) (specialized service used for obtaining collective technical requirements as a package, to form organizations such as a virtual hospital); children health information (CHI) (a service developed to address children with emotional, behavioral or mental health problem and their family members); Semantic medical access (SMA) (application that employs medical rule engines to analyze massive amounts of sensor data stored in the cloud); indirect emergency healthcare (IEH) (service that can offer many solutions, such as information availability, after notification, post-accident action, and record keeping); embedded gateway configuration (EGC) (allows for automated and intelligent monitoring by employing a medical sensor network based on the IoT and personal mobile gateway); and embedded cost prediction (ECP) (a service for ubiquitous healthcare that applies IoT-enabled remote health with a context predictor for patients).

All those devices and processes can be named under the label Remote Health Monitoring (RHM), which continuously stores persons' health data, allowing health workers not only to what happens in real time, but also what is supposed to

---

[13] SWAROOP, K. Narendra et al. A health monitoring system for vital signs using IoT. **Internet of Things**, v. 5, n. 2019, p. 116–129.

[14] MELCHERTS, Helga E. The Internet of Everything and Beyond: the Interplay between Things and Humans In DIXIT, Sudhir (ed.). **Human bond communication:** the holy grail of holistic communication and immersive experience. Hoboken: John Wiley & Sons, Inc., 2017, p. 439.0-468.0; p. 459.

[15] MILOVANOVIC, Dragorad; BOJKOVIC, Zoran. Cloud-based IoT healthcare applications: Requirements and recommendations. **International Journal of Internet of Things and Web Services**, v. 2, 2017, p. 60-65.

happen.[16] Heart rate, pulse rate, blow pressure, patient's temperature, respiratory rate, as well as medication and diet monitoring, are parameters that can be catch in the data flow providing elementary analysis so as to enable progress of expectations of a health program and/or treatment in real time. Then, RHM can improve physicians abilities to manage and monitor patients in innovative healthcare settings, utilizing advanced methods to gather health information from the patient's common environment, transmitting data to healthcare providers in different places to analyze and recommend programs for better health or disease control. This way, faster diagnosis and decision-making are enabled by compiling several data.[17]

There are several technological issues that have to be solved before the liberation the full potential of such technologies, though.[18] Accurate data acquisition, bandwidth, interoperability between hardware and software, limitation of battery life, biocompatibility of sensors - beside delivery of good health services - are the main ones (not to mention security and privacy issues, that will be approached lately here).

Based on the possibilities IoT (which, when applied to medical and health issues can be named *Internet of Medical Things*, or IoMT), in 2015 the president Barack Obama (USA) launched the *precision Medicine Initiative*, aiming to improve therapies by a "tailoring" of prevention and treatment strategies in order to fit the specifics of each individual patient.[19] This means the recognition, by politics, of a new paradigm in healthcare, in which the "one size fits all" treatments is substituted by a totally individual and specific approach, which has a potential to make diagnosis and treatments much more precise than currently.

Not only for faster, more precise and remote diagnosis and treatments could IoMT contribute: the huge amount of data could be read for discoveries of diseases such as cancer and other genetical diseases. When environmental and lifestyle measurement (which can be measured and registered by simple devices such as wearables) is added to genomic profiles (which could be, in the future, also developed by IoMT devices and strategies, such as automated DNA sequencers), such complex diseases (that

---

[16] GUNTUR, Sitaramanjaneya Reddy; GORREPATI, Rajani Reddy; DIRISALA, Vijaya R. Internet of Medical Things: remote healthcare and Health Monitoring Perspective In: HASSANIEN, Aboul Ella; DEY, Nilanjan; BORRA, Surekha. **Medical Big Data and Internet of Medical Things:** advances, challenges and applications. Boca Raton: CRC Press, Taylor & Francis Group, 2019, p. 633-703; p. 637-638.

[17] GUNTUR, Sitaramanjaneya Reddy; GORREPATI, Rajani Reddy; DIRISALA, Vijaya R. Internet of Medical Things: remote healthcare and Health Monitoring Perspective In: HASSANIEN, Aboul Ella; DEY, Nilanjan; BORRA, Surekha. **Medical Big Data and Internet of Medical Things:** advances, challenges and applications. Boca Raton: CRC Press, Taylor & Francis Group, 2019, p. 633-703; p. 640-641.

[18] GUNTUR, Sitaramanjaneya Reddy; GORREPATI, Rajani Reddy; DIRISALA, Vijaya R. Internet of Medical Things: remote healthcare and Health Monitoring Perspective In: HASSANIEN, Aboul Ella; DEY, Nilanjan; BORRA, Surekha. **Medical Big Data and Internet of Medical Things:** advances, challenges and applications. Boca Raton: CRC Press, Taylor & Francis Group, 2019, p. 633-703; p. 688-689.

[19] BOROVSKA, Plamenka. Big Data Analytics and Internet of medical Things Make Precision Medicine a Reality. **International Journal of Internet of Things and Web Services**, v. 3, 2018, p. 24-31.

have diagnosis that depend on a complex of factors) can be studied in a much more precise database.[20] It can be imagined that, when added to other technologies such as machine learning and artificial intelligence (AI), IoMT, big data analytics and cloud computing could deliver together, then, not only treatments, diagnosis and prognosis, but also deep and life-important knowledge.

There are also examples of applying IoT to formal education, informal learning and structural training - specially in complex situations involving teamwork, which is very important for improving qualities in healthcare services delivery. Bannan, Gallagher and Lewis[21] consider that in the space of emergency training simulations (historically limited either to fully live-action human observable field-basis simulation and computer simulations), IoT opens innovative, hybrid digital-physical opportunities for delivering and for understanding outcomes of training and education efforts in a more comprehensive way, offering new insights and methods in the challenges of training new healthcare professionals.

All those promises in technology are formidable, then, from the point of view of the health as a fundamental right. And if we consider the constitutional regulation of such fundamental right in Brazilian current Constitution, they have a huge potential for actualizing what article 196[22] enforce about that right. They could also help actualizing article 198, II of Brazilian Constitution,[23] which enlists integral care and prevention as corollaries for healthcare services. Enlisting health as a fundamental right in Brazil in 1988 Constitution is a very criticized matter because of the lack of effectiveness it has in practice. As said by Bulos,[24] Public Authorities charged with carrying out the constitutional message, have not considered the principle of universal and isonomic treatment, according to the current stage of medical science. Thus, such norm has not had any concrete effect, because in Brazil, access to health is proportional to the economic situation of the person. And, as explained by Nascimento,[25] there are no public policies capable of conferring such right to all the population, due to the wrecking of the Brazilian Unique Health System (Sistema Único de Saúde, SUS); as consequences of

---

[20] BOROVSKA, Plamenka. Big Data Analytics and Internet of medical Things Make Precision Medicine a Reality. **International Journal of Internet of Things and Web Services**, v. 3, 2018, p. 24-31.

[21] BANNAN, Brenda; GALLAGHER, Shane; LEWIS, Bridget. Next-Generation Learning: Smart Medical Team Training In: GENG, Hwaiyu. **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 222-249; p. 222-223.

[22] "Health is the right of all and the duty of the State, guaranteed by social and economic policies aimed at reducing the risk of disease and other aggravations and universal access to actions and services for their promotion, protection and recovery".

[23] "Integral care, with priority for preventive activities, without prejudice to the care services".

[24] BULOS, Uadi Lammêgo. **Constituição Federal Anotada.** 11 ed. rev. atual. São Paulo: Saraiva, 2015, p. 1436.

[25] NASCIMENTO, Carlos Valder do. Direito fundamental à saúde. In: MARTINS, Ives Gandra da Silva; MENDES, Gilmar Ferreira; NASCIMENTO, Carlos Valdez do (org.) **Tratado de Direito Consstitucional.** 2 ed. São Paulo: Saraiva, 2012, p. 379-437; p. 391.

such impoverishment, the wealthiest ones hire health insurance companies, while the poorest ones receive discriminatory treatment (long lines, bad-delivered services, lack of medicines and machines, etc.).

In the wake of those important criticisms, IoMT added to other *avant-garde* technologies could help actualizing such right because: i) technologies such as wearables, sensors, smartphones and smartwatches are becoming each day more popular and economically accessible (then, they would be means for facilitating communication between patients and healthcare State institutions); ii) they could make healthcare service much better delivered (both in speed and quality); iii) the duty of the State to provide a better service would become easier not just with the creation of newer institutions, but also with politics of incentives for citizens to acquire gadgets (which would also benefit technology companies and financial institutions/banks, for example); iv) reduction of risks of diseases and prevention would be much more effective with remote monitoring, which would save the State huge amounts of resources that would be spent with remedies, treatments, surgeries, etc.

It can be preliminary concluded, then, that IoT (and IoMT) have potential to revolutionize healthcare services and systems through application and improvement of everyday devices and techniques (such as wearables, cloud computing and internet-based communication) in addition to other yet sophisticated techniques (machine learning, artificial intelligence, big data analysis and genetic automated mapping) in order to collect/analyze data and, with such structures, make better diagnosis, prognosis, prevention and treatment. But several technical, ethical and juridical concerns have worried scholars that see this interesting technical field as promising.

It is very visible that IoT when applied to medical issues has a huge potential to enhance healthcare services, then. But when the issue is communicating personal information through electronic networks, security issues - such as risks of leaking data, system invasions and a huge plethora of crimes concerning to individuals' honor and privacy - and this is why such risks and insecurities must be approached.

3. RISKS AND UNCERTAINTIES OF THE IOT CONCERNING THE SECURITY OF ITS USAGE

Security is the first main concern about using IoT/IoMT. As gadgets and devices are connected to the net, the risk of viruses, malwares and hacker invasions constantly worries researchers and scholars - not as a simply potential risk, but as a real menace. To illustrate this fact, for example, in October 2016 the first malware to invade IoT was introduced in the world, able to infect connected devices; it easily accessed devices by using default login information of users, turned those devices into Botnet for DDoS (Distributed Denial of Service) attacks that brought many service websites to stop

working for hours (including big hosting companies); that malware is available as open source for modification - which made a modified version of the malware be introduced after some hours of the main attack.[26]

The use and evolution of IoT depend mainly on the security aspect, as now the security measures should control the actions both of users and objects. In parallel, being its devices characterized by constrained computing resources, it is impossible to use conventional security mechanisms. Moreover, heterogeneity and the multiple interconnections of devices produce huge amounts of data that are hard to manage.[27]

Unfortunately it is utopian to believe in a total security for any system, as there is always likelihood of dangers or threats and new vulnerabilities arising everyday.[28] But it is important to highlight that for IoMT, security is essential, because a single insecure point in a system of healthcare costs a human life. Negash et. al[29] report, for example, that an insulin pumper in a system of management of glucose based on IoMT can be hacked within 100 feet; then, gateways and sensor nodes must be highly considered, because if only one of the devices/components is hacked, the entire system can be manipulated (or even controlled) by invaders.

Likewise, hacked data could fall into the hands of people with dubious intentions. An insurance company, for example, could illegally collect information concerning its customers' health - which could show that the forces who should originally be working toward the well being and health of patients could end up turning against him/her.[30]

Taking into consideration that (real and hypothetical) concerns, then, it has been suggested that a solid security system ought to incorporate verification procedures and advancements, confirming supplier and patient identifier in order to guarantee gadgets are used by approved personnel, as well as interconnections between devices must be secured by advanced processes and protocols.[31] It is important to point out that, as healthcare frameworks process and store extremely delicate information - and,

---

[26] SHARMA, Neha; SHAMKUWAR, Madhavi; SINGH, Indjerit. The History, Present and Future with IoT In: BALAS, Valentina et al. (ed.). **Internet of Things and Big Data Analysis for Smart Generation**. Cham: Springer, 2019, p. 101-160; p. 141.

[27] GRAMMATIKIS, Panagiotis I. Radoglou; SARIGIANNIDIS, Panagiotis G.; MOSCHOLIPS, Ioannis D. Securing the Internet of Things: Challenges, threats and solutions. **Internet of Things**, v. 5, 2019, p. 41–70.

[28] SÁNCHEZ, Julia et al. Security in Smart Grids In: SUN, Hongjian; WANG, Chao; AHMAD, Bashar I. (ed.). **From Internet of Things to Smart Cities:** Enabling Technologies. Boca Raton: Taylor & Francis, 2018, p. 433-547; p. 440.

[29] NEGASH, Behailu et al. Leveraging fog computing for healthcare IoT In: RAHMANI, Amir M. et al. **Fog computing in the Internet of Things:** intelligence at the edge. Cham: Springer, 2018, p. 336-395; p. 355.

[30] ROXIN, Ioan; BOUCHERAU, Aymeric. Introduction to the technologies of the Ecosystem of the Internet of Things In BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 104.0-193.0; p. 174.4.

[31] GUNTUR, Sitaramanjaneya Reddy; GORREPATI, Rajani Reddy; DIRISALA, Vijaya R. Internet of Medical Things: remote healthcare and Health Monitoring Perspective In: HASSANIEN, Aboul Ella; DEY, Nilanjan; BORRA,

in this sense, not only technical solutions (i.e. encryption and ID administration) must be developed, but regular activities (i.e. purchaser support, divulgence, open mindfulness, customer instruction, socio-ethical based customer rights, security accreditation, responsibility based self-direction, transparency, accumulation constraint, shopper assent, etc.) have also to be included.

One of the main reasons behind the vulnerabilities of IoT is concerning to its main characteristic: the vulnerability of devices that form it, the high-constraining level of the resources of many devices, and the decentralization of the designs can be enlisted here. The ubiquity of the IoT also makes huge amounts of information easily available for invaders. And finally, the establishment of trust among actors in a such decentralized net is another important problem - which demands the development not only of technical schemes (such as context-aware architectures and cryptography), but also security policies such as deployment of reputation schemes enabling devices to decide concerning the level of trust that can be dedicated to other actors interaction with them.[32]

Aly et al[33] describe main menaces to the usage of IoT in society, systematizing them as it follows. In first place, it must be informed that there will be several challenges to forensics in the IoTs environments - as with the increasing of insertion of such technology in common life, people will probably start suing one each other based on their behavior in the IoT and on security characteristics of devices/networks of people. For start facing those challenges, device level forensics (which involves collecting potential digital evidence from the participating physical IoT devices such as audio, video, memory, graphics, etc.), cloud forensics (that is because, as the evolution of the sophisticated security threats from devices where most data generated is being moved to the Cloud, forensics strategies have to be adapted to that domain as well), and network forensics (for in network environments, potential attack logs can be extracted and used to conduct the digital investigation process, such as industrial networks, home networks, LANs, WANs, MANs, etc.) have to be developed.

Another important field of undesired attacks to IoT is related to the unexpected data usage. The widespread usage of ubiquitous computing enabled by IoT technologies, has been noticeably pervasive. Daily routine, habits, general health data are private informations that could be inferred from presumably even from non-critical data.

Surekha. **Medical Big Data and Internet of Medical Things:** advances, challenges and applications. Boca Raton: CRC Press, Taylor & Francis Group, 2019, p. 633-703; p. 684-685.

[32] TSIATSIS, Vlasos. **Internet of Things:** technologies and applications for a new age of intelligence. 2 ed. London: Academic Press, 2019, p. 478.

[33] ALY, Mohab et al. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. **Internet of Things**, v. 6, 2019, p. 1-24.

Technical limitations of IoT devices when faced to the computational complexity put another technological problem for IoT, as resources such as memory, computation, and energy, are limited in IoT devices and create a crucial bottleneck in the adoption of security measures for real-time on-board implementations. Interoperability of security protocols for each layer of security in global IoT have also to be developed, combining effectively security standards at each layer.

Because of the heterogeneity of networks, architectures and protocols, IoT paradigm devices, clouds and networks become even more vulnerable to single points of failure than any other paradigm. Then, IoT requires mechanisms and standards to introduce redundancy while keeping in view the trade-off between costs and the reliability of the entire infrastructure.

Trusted updates and management are also a very important failure issue for security in IoT smart devices. Such matter has to be regulated by a complex governance that has to be developed for IoT, and blockchain technology could be combined to it for making safety available in such domain, but even that technology puts other challenges to IoT. Despite providing robust approaches for securing IoT, the blockchain systems are also vulnerable, because the consensus mechanism depending upon the miner's hashing power can be compromised, thereby allowing attackers to host the blockchain. And private keys with limited randomness can be exploited to compromise the blockchain accounts.

Another very complex challenge put by IoT is the autonomy devices can acquire with its development, as pointed out by Sfar et al.[34] That autonomy enable objects to participate actively, recognizing events, changes in their environment, and react without human intervention. It can be said that networks, instead of simply linking communication between points and processing data, are expected to become intelligent and capable of perceiving, sensing and acting, recognizing, acting and reacting. Then, IoT security must also acquire greater autonomy in perceiving threats and reacting to attacks, based on a cognitive, systemic approach.

Moreover, ubiquity of IoT raises legitimate questions about human privacy, and how to cope with the heterogeneity of user and application requirements in terms of security services. This requires developing adaptive, context-aware and user-centric security solutions. This diversity in terms of security requirements can be addressed via the adaptive, context-aware management of security profiles and policies.

Legally speaking, security has to be taken in the highest account as well - not only because of the importance of the fundamental right to health and life (as pointed out above), but also to avoid prosecutions, lawsuits and extenuating bureaucracy to actualize rights in practice. Both consumers and suppliers have to be protected from

[34] SFAR, Arbia Riahi et al. A roadmap for security challenges in the Internet of Things. **Digital Communications and Networks**, v. 4, n. 2, , p. 118-137, abr. 2018.

time-consuming lawsuits that can explode in number, as class actions and product liability lawsuits (among several others) could be brought against IoT manufacturers and other stakeholders (i.e. application developers) by affected consumers.[35]

Regulation and governance of IoT/IoMT have also to be delicately and detailedly discussed before full implementation of such technology in everyday life of millions of patients/citizens. Being the main interested actors in enhancing of health/life, citizens have to take part in the regulation processes, even though huge private companies have driven the development and evolution of IoMT. Then, the management of its regulation should be with the support by all (i.e. governments, private sector, civil society and international organizations), and not only under the control of one single organization (i.e. the ICANN). Furthermore, non-discriminatory access and transparency must be elected as fundamental principles for the governance of IoT, as well as accountability. Transparency and non-discriminatory access can mobilize civil society to influence constitutional and architectural principles of a regime of governance, and also foster the stability of the developed legal framework. And accountability improves the governance regimes of organizations.[36]

It was seen, then, that there are many possibilities of breaking a system in order to collect personal information obtained and stored through IoT/IoMT systems. It was also seen that scholars have been concerned not only with technical solutions for those problems, but also to regulating strategies (such as new types of legal principles) in order to better regulate preventively and responsively those technologies. But there still are very important legal observations concerning to fundamental right to privacy and how it is being considered regarding to such regulatory strategies.

4. FUNDAMENTAL RIGHT TO PRIVACY AND THE INTERNET OF THINGS: ETHICAL AND JURIDICAL CONSIDERATIONS

Some of the worries related to data we can find in the internet are increased in IoT. Allhoff and Henschke[37] study that issue from the possibilities of building a profile of users: smart homes, for example, could show the routines, consuming habits and other current information about people who use such technology - and that information is communicated back to the manufacturers (being that not all of that information is even encrypted). It means that not only the market could have access to such data, but also that hackers could make use of such information for bad purposes (making possible

[35] MARAS, Marie-Helen. Internet of Things: security and privacy implications. **International Data Privacy Law**, v. 5, n. 2, p. 99-104, 2015, p. 102.

[36] WEBER, Rolf H. Internet of things – Need for a new legal environment? **Computer Law & Security Review**, v. 25, p. 522–527, 2009, p. 526-527.

[37] ALLHOFF, Fritz; HENSCHKE, Adam. The Internet of Things: Foundational ethical issues. **Internet of Things**, v. 1–2, p. 55-66, 2018.

that intimate aspects of a person's life). According to the authors, Europe has already enforced its General Data Protection Regulation (GDPR) since mid-2018, and in Courts around the USA the right to digital privacy has started to be recognized, but IoT is still mostly unregulated - but there are lots of pitfalls to privacy which are disposable to bad intentioned third parties.

The unauthorized use of private health information could present huge security risks to the patients. Then, compact smart sensors that record, store and transmit to a server demand secure approaches.[38] Ensuring privacy must not be only a matter of specialized arrangements (i.e. encryption, ID administration and security upgrading). The prerequisites of IoMT communication systems in healthcare applications are interoperability (which is expected to empower diverse things to cooperate to give the desired benefit), bounded idleness and reliability (which should be concerned when managing emergency circumstances in order for the intercession); furthermore, authentication, security, privacy and respectability use be compulsory when sensitive information is exchanged over the effective.

Health conditions - which could comprehend since simple and current information such as mood, stress level, demographics (e.g., gender, marital status, job status, age), smoking habits, overall well-being, personality type, levels of exercise, types of physical activity or movement, until serious and sensible information, such as progression of Parkinson's and/or Alzheimer's disease, HIV, cancer, epilepsy and schizophrenia - could be inferred from data analysis hugely collected by IoMT devices.[39] Such informations could be manipulated to build an unwanted user's profile, which would be very useful for health insurance and pharmaceutical companies. The devices could also be used for eavesdropping by third parties, and all such problems concerning to privacy could erode consumers' confidence on such technology.

Moreover, as IoT is a digital technology, ethical aspects must be consider to its design and use from a digital perspective. The digital actors are all stakeholders (i.e. designers of IoT devices/services, standardization and governing bodies, vendors and users). Then, a normative digital ethics must be developed to define moral standards for IoT design and operation by analyzing the impact of reliability, security, data ownership and traceability, user consent, compliance to legal and regulatory requirements and social values.[40]

---

[38] GUNTUR, Sitaramanjaneya Reddy; GORREPATI, Rajani Reddy; DIRISALA, Vijaya R. Internet of Medical Things: remote healthcare and Health Monitoring Perspective In: HASSANIEN, Aboul Ella; DEY, Nilanjan; BORRA, Surekha. **Medical Big Data and Internet of Medical Things:** advances, challenges and applications. Boca Raton: CRC Press, Taylor & Francis Group, 2019, p. 633-703; p. 682.

[39] SOLANGI, Zulfiqar Ali et al. **The future of data privacy and security concerns in Internet of Things** *In:* 2018 IEEE INTERNATIONAL CONFERENCE ON INNOVATIVE RESEARCH AND DEVELOPMENT (ICIRD), 11-12 May 2018, Bangkok. Available at: https://ieeexplore.ieee.org/document/8376320. Access in: Jun 24 2019.

[40] CHAUDHURI, Abhik. **Internet of things, for Things, and by Things**. Boca Raton: CRC Press, Taylor & Francis Group, 2018; p. 135.9-137.2.

In order to utilize the full potential of the IoT, national and international legislation needs to be complied too. Storing sensitive personal data for healthcare in a system demands that data privacy laws get complied to it. The system should enable storing sensitive data in a way that preserves confidentiality and privacy according to ethical/legal principles. Furthermore, enabling data protection in the system will be an essential part of ensuring the compliance of the system with relevant international and national legal standards.[41]

The ability to collect a constant and regular flow of personal information, from a privacy perspective, may cause significant privacy risks to users.[42] Collected information could reveal locations, habits, and physical conditions of an individual over time. If shared without proper restrictions, this information could be reused for unknown purposes, shared with unscrupulous third parties, or retained even when it is no longer relevant at the individual's circumstances have changed.

The more data is collected, the more risk there is that it may be used for different purposes. Then, there is a principle called *data minimization*, which can be found throughout several privacy frameworks addressing protection of data and policy initiatives. Such principle refers to a limitation of data that companies should collect, retain and disposed securely once the information is no longer needed.[43] In this sense, a balance is needed between developers and users of IoMT services in their goals of collecting personal information, being pointed out that data collection practices must be a basis for developing data minimization policies. Data minimization acquires a renewed importance when we analyze that retaining large amounts of data can tempt IoMT service provider to sell such information to interested third parties (i.e. insurance and marketing companies).[44]

In the emerging market of IoT, a consensus between the industrial actors in the domain must arrive, many concerning to compatibility between products to communicate and exchange data. Nowadays, each company uses its own technological solutions. Task forces from several manufacturers have recently discussed standards for IoT, in order to allow devices to mutually understand each other and determine the requirements regarding connectivity and interoperability. Standardization is central in the case of a need for technological convergence. The notions of norms and standards

---

41 MELCHERTS, Helga E. The Internet of Everything and Beyond: the Interplay between Things and Humans In DIXIT, Sudhir (ed.). **Human bond communication:** the holy grail of holistic communication and immersive experience. Hoboken: John Wiley & Sons, Inc., 2017, p. 439.0-468.0; p. 449.

42 GILBERT, Françoise. Privacy and Security Legal Issues In: GENG, Hwaiyu. **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 1582-1636; p. 1587-1588.

43 GILBERT, Françoise. Privacy and Security Legal Issues In: GENG, Hwaiyu. **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 1582-1636; p. 1596-1597.

44 GILBERT, Françoise. Privacy and Security Legal Issues In: GENG, Hwaiyu. **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 1582-1636; p. 1600-1601.

are present in Europe, and in America under the same name: a norm is a frame or reference published by an official international organization for standardization (i.e. ISO, ECS, AFNOR, IEEE); a standard is group of recommendations advocated by a group of representatives and informed users that is widely disseminated and used. HTML format for the web is the prime example of this type of procedure.[45]

Nowadays, the fundamental right to private life collides with the omnipresence of the Internet and pervasive computing; individuals communicate and exchange between pairs displaying a desire for collaboration rather than exclusion.[46] Because of such important changes in private life, a general principle to guide the development of the IoT was issued by the European Commission:[47] *the security of information and the protection of private life* must be part of the basic requirements for IoT (and related) services. Service providers must deploy the necessary means to guarantee the security of the information and devices during the setting up of their applications, and they must preserve the confidentiality of the information they possess as well.[48]

Although establishing norms and standards is very important, it must be recognized that the development of connected devices and services raises unprecedented problems in regard to regulation, mainly related to novel situations that are not subject to the current legislation or even to any current regulatory body. Because the relatively rapid IoT growth (according to the estimates,[49] there will be several billion connected devices by 2020), a judicial and technological framework is all the more important.[50]

Major companies (such as IBM, Intel, Ericsson, Samsung or Microsoft) have created several international organizations around them to ensure regulatory functions, such as the *IoT Security Foundation* (nonprofit organization that approaches security aspects of the IoT) and the *Open Connectivity Foundation* (which proposes better interoperability between devices originating with different manufacturers). Nevertheless, both

---

[45] BOUHAÏ, Nasreddine. The IoT: Intrusive or Indispensable Objects? In BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 10-42; p. 18.6-19.5.

[46] ROXIN, Ioan; BOUCHERAU, Aymeric. Introduction to the technologies of the Ecosystem of the Internet of Things In BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 104.0-193.0; p. 163.7.

[47] DIGITAL AGENDA FOR EUROPE, IoT Privacy, Data Protection, Information Security, A Europe 2020 Initiative, 2013.

[48] ROXIN, Ioan; BOUCHERAU, Aymeric. Introduction to the technologies of the Ecosystem of the Internet of Things In BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 104.0-193.0; p. 164.6.

[49] ROSE, Karen.; ELDRIDGE, Scott D.; CHAPIN, Lyman. The Internet of Things: an overview. **The Internet Society (ISCO)**, 2015. p. 8.

[50] ROXIN, Ioan; BOUCHERAU, Aymeric. Introduction to the technologies of the Ecosystem of the Internet of Things In BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 104.0-193.0; p. 169.5.

multidisciplinary and multi sectorial regulation is necessary to standardize the IoT development at the international level (the same way the Internet was regulated).[51]

In order to guide the regulation of data obtained and stored by devices, Holdowsky et al[52] enlisted four basic principles, as it follows: i) knowledge and choice (users must be notified when the data collection occurs, and must be able to decide about the recording); ii) the purpose of the data collection and usage limitations (companies must notify the user and explain the purpose of the operation whenever they collect data of users - and business must also commit to use the data only in a limited way, with the knowledge of the user); iii) minimization (business must only recover what is necessary for its service to function, when they collect data from users); iv) responsibility and security (data are private and belonging to the user - thus, business are responsible for what they collect and must use it with all the possible care to guarantee data security against third-part interference).

Weber[53] has pointed out that a new legal environment is necessary for IoT/IoMT, advocating for better security environments and higher confidentiality standards, as privacy and data protection are especially important for maintaining privacy in IoT. This is why, as well, new regulatory approaches to ensure security and privacy are needed - and, particularly, practices such as interception of attacks, data authentication, access control and guarantee of privacy of consumers.[54] But not only the establishment of legal principles must be emphasized: the nature of IoT demands a differentiated, heterogeneous legal frameworks, which must take into account the technicity, globality, ubiquity and verticality of IoT. The limited national legislation is not appropriated to such context, but self-regulation would also not be enough to ensure security and privacy. Then, internationally established substantial key principles is defended by the author.

Industry standards also must be created, in order to limit the collection and use of data relating to sensible information (health, religion, sexual orientation, etc.).[55] Processing and storing sensible data by IoT devices, clouds and networks require express consent of concerned individuals, and this should be done with adequate measures to ensure that the data collection are uniquely belonging to the concerned individual.

---

[51] ROXIN, Ioan; BOUCHERAU, Aymeric. Introduction to the technologies of the Ecosystem of the Internet of Things In BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 104.0-193.0; p. 169.5-170.5.

[52] HOLDOWSKY, J. et al. **Inside the Internet of Things (IoT)**. Westlake: Deloitte University Press, 2015.

[53] WEBER, Rolf H. Internet of things – Need for a new legal environment? **Computer Law & Security Review**, v. 25, n. 6, p. 522-527, nov. 2009.

[54] WEBER, Rolf H. Internet of Things – New security and privacy challenges. **Computer Law & Security Review**, v. 26, n. 1, p. 23-30, jan. 2010.

[55] WEBER, Rolf H. Internet of things: Privacy issues revisited. **Computer Law & Security Review**, v. 31, n. 5, p. 618-627, dec. 2015.

Protecting personal data demands self-regulation on the part of consumers. From that perspective, individuals should be able to control and choose which data are collected, by who and when such collection occurs, as the IoT basically is a repository for every aspect of an individual's life - then, its applications should facilitate the rights of accessing, modifying and deleting personal data.[56] Moreover, the consent users provide for using IoT devices, as well as data collected by such gadgets ought to be informed, freely given, and users should not be economically penalized - or even have degraded access to capabilities of their devices - if they decide not to use a specific service.

A policy of data minimization (through periodical deletion of no longer needed data, as well as of storing data only as needed) must be practiced, in order to reduce harm associated with data breaches and to minimize the risk of deviated usage. But even self-regulation and well developed data policies (which would be embedded in the devices' operational systems themselves) are not enough: privacy must be recognized as a human right, as it occurs in many law systems around the world - and that human right must have serious reflections even on self-regulation systems and policies.

When analyzing juridical and ethical questions concerning to subcutaneous chips to collect medical information (a technology that could also be used for IoMT - and even if it would not, there are analogous characteristics between both technologies), Matos, Menezes and Colaço[57] enlist a series of principles for safety of sensible personal data:

a) correlation in collection and processing informations;

b) accuracy of collected data (sided by the obligation in its updating);

c) function of collecting (being that such function must be known before collection) - and that principle can be divided into other three principles: i) pertinency (the collection must be specified in the relationship between collected data and the intended purpose); ii) non-abusive use (the collection ought to be specified in the relationship between the function of collection and the usage of its data); iii) right to oblivion (elimination or putting into anonymity of data that are not necessary anymore);

d) publicity (there must be a a public database concerning to personal information);

e) personal access (the individual must have personal access to information collected about him/herself in order to obtain copies, correcting wrong information, integrating the incomplete ones and eliminating the illegally obtained ones);

---

[56] MARAS, Marie-Helen. Internet of Things: security and privacy implications. **International Data Privacy Law**, v. 5, n. 2, p. 99-104, 2015.

[57] MATOS, Liliane Gonçalves; MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Limites à implantação de chips subcutâneos: a tutela da privacidade como instrumento de proteção da pessoa na sociedade da informação. **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 18, n. 3, p. 267-300. set./dez. 2017.

f) logical/physical collection of data.

According to the authors (and inspired in Rodotà),[58] that principological basis can enable juridical thought about dealing data - in which the negative/passive posture about data protection could be substituted by a positive/dynamic position. The juridical technique about data protection also changes - from a repressive capability, given to the private individual only after violation, to a direct and continuous power to control data collectors, independently of the existence of an actual violation. But that basis of new principles would not be enough, by itself, to protect sensible data. Such basis must be associated to those contained in the Brazilian Civil Rights Framework for the Internet (Lei n. 12.965/2014) and, mainly, to the unity of the juridical system through the collation of fundamental and human rights.

Juridically speaking about constitutional privacy (which is institutionalized in article 5, X, of Brazilian Constitution of 1988), Ávila and Woloszyn[59] highlight an important theoretical difference between the notions of *privacy, intimacy* and *secrecy* (which are imbricated, but not synonymous). Such notions are differentiated by the degree of exclusivity the individual confers to the information: this way, *privacy* comprehend the widest scope of the three, and regards to those informations related to familiar, laboral and communitarian environments (which are safe from unwanted publicity according to the will of its titular); *intimacy* has a narrower scope, in which there are informations about the individual which he/she intends to keep in secrecy. In this sense, intimacy is the essential nucleus of the privacy - and neither privacy nor intimacy can be changed by infra constitutional norms (or even by new amendments). *Secrecy*, by its turn, is contained in other norm (article 5, XII), and regards to those information that are private, but which Brazilian Constitutional Law provides the possibility of disclosure with a judicial writ such as financial and some professional informations).

It is important to highlight that when the Constitution was promulgated, cellphones and the internet were not part of the reality, and so, it would not be fair to make a strict/literal interpretation of such possibilities of privacy, intimacy and secrecy. The new reality must be studied in order to make a new legal framework and new principles related to such important fundamental rights.

In order to supply such void, in 2018 Brazil has enforced a *Personal Data Protection General Act* (Lei 13.709/2018), aiming to, among other goals, restrict activities regarding to personal data processing, being that, to be considered totally legal, a group of norms must be observed by service providers. In its article 6, a group of principles is

---

[58] RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Coord. Maria Celina Bondin de Morais. Translation to Portuguese by Danilo Doneda e Luciano Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 60.

[59] ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, Curitiba, v. 4, n. 3, p. 167-200, set./dez. 2017.

enlisted and enforced: *finality, adequacy, necessity, free access, quality of data, transparency, security, prevention, non-discrimination,* and *accountability.* Of all those principles, Mulholland[60] highlights that finality and non-discrimination are the most important ones concerning to sensible data.

Finality principle preconizes that data must be processed for predetermined purposes, which must be explicitly pre-informed to the data owner, and with severe restrictions to ulterior usage for other functions. Non-discrimination principle, by its turn, establishes prohibitions for using personal data in order to illegally or abusively discriminate people. When law related discrimination to illicitness and abusiveness, it seems to recognize possibilities of distinctive treatment to people from data analysis, as long as it is not illegal or abusive - or, in other words, it would be possible to distinguish people when making, for exemple, data mining, but without *excluding* people from dignity. Then, it would be legally possible, for exemple, to classify people according to their age, for exemple to calculate prices of car insurance; however, when such classification is related to sensible data (such as genetics, health conditions, sexual behavior, etc.), which are part of people intimacy, an interpretation parallel to constitutional meanings must be done. In this sense, in another exemple, insurance companies could not explore sensible data of people who have a genetical predisposition to cancer, or a sexual behavior that is considered of high risk, in order to charge them extremely high fees (to the point that they could not afford such insurances).

The same legal act defines, in its article 5, I and II, the differences between *personal data* and *sensible personal data.* The first one regards to natural persons, while the second one is related to race, ethnicity, religious orientation, political opinion, affiliation to labor union or religious, philosophical or political organization, data regarding to health conditions or sexual life, genetic or biometric data, when linked to a natural person.

It must be said that the Act promotes a very strong importance to consenting of the owner of data to admit the processing - in other words, when he/she manifests free, informed and unmistakeable consent for a legally determined finality (article 5, XII); moreover, such consent must be realized in a highlighted and specific form (article 11, I). Then, it seems to be very protective and parsimonious when regarding to contractual freedom about sensible data. However, it permits processing sensible data without free consent when it is indispensable for executing public policies provided by law (article 11, II, *b*). Certainly, an unconstitutionality can be seen here, as the State could promote discrimination of certain groups (for exemple, in social security public policies) without consent of the owner of sensible data, for exemple.

---

[60] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: Uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitó ria, v. 19, n. 3, p. 159-180, set./dez. 2018.

And this is the neuralgic point of Brazilian legislation concerning to privacy and public policies of healthcare enhancement through IoMT: if such unconstitutional legal dispositive get enforced in this area, not only Brazilian government will be potentially causing discrimination, but also, letting an open pitfall for security in public services involving IoT.

5. CONCLUSION

After all that argumentation, it can be concluded that IoT, when applied to medical issues, plays a fundamental role in remote healthcare, increasing efficient usage of health devices, and improving accessibility of healthcare services. Moreover, several useful devices for that technologies (such as smartphones, wearables and sensors) are already available and very popular among consumers, and with the passing of times, they can be increasingly used by elderly people (who needs the most health monitoring because of age and chronicle diseases). Admissions in healthcare institutions could be reduce, and this is a fact that potentially could reduce public spendings on healthcare (as a physical institution would not be needed for several patients anymore).

All those potentials and much more are really admirable from the point of view of actualizing health as a fundamental right. And when Brazilian constitutional regulation of such fundamental right is considered. IoT/IoMT could enhance healthcare services, then. But when the issue is communicating personal information through electronic networks, security issues (i.e. leaking data, system invasions and crimes concerning to individuals' honor and privacy) must be considered.

Hacked data could fall into the hands of people with deviated intentions. Health insurance companies and governments could illegally collect information concerning its customers' health - which could show that the forces who should originally be working toward the well being and health of patients could end up turning against him/her. And all risks are aggravated when we analyze that IoT/IoMT are characterized by ubiquity, collecting all types of personal data (including sensible ones) 24/7.

As healthcare frameworks process and store extremely delicate information - and, in this sense, not only technical solutions (encryption and ID administration, for exemple) must be developed, but regular activities (consumer support, divulgence, open mindfulness, customer instruction, socio-ethical based customer rights, security accreditation, responsibility based self-direction, transparency, accumulation constraint, shopper assent, etc.) have also to be included.

Security has to be taken in the highest account not only because of the importance of the fundamental right to health and life, but also to avoid prosecutions, lawsuits and extenuating bureaucracy to actualize rights in practice. Both consumers and suppliers have to be protected from time-consuming lawsuits that can explode in

number, as class actions and product liability lawsuits (among several others) could be brought against IoT manufacturers and other stakeholders (i.e. application developers) by affected consumers.

Regulation and governance of IoT/IoMT have also to be delicately and detailedly discussed before full implementation of such technology in everyday life of millions of patients/citizens. Being the main interested actors in enhancing of health/life, citizens have to take part in the regulation processes, even though huge private companies have driven the development and evolution of IoMT. Then, the management of its regulation should be with the support by all (i.e. governments, private sector, civil society and international organizations), and not only under the control of one single organization.

Ensuring privacy must not be only a matter of specialized arrangements. Health conditions could be inferred from data analysis hugely collected by IoMT devices. Such informations could be manipulated to build an unwanted user's profile, which would be very useful for health insurance and pharmaceutical companies. The devices could also be used for eavesdropping by third parties, and all such problems concerning to privacy could erode consumers' confidence on such technology. Collected information could as well reveal locations, habits, and physical conditions of an individual over time. If shared without proper restrictions, this information could be reused for unknown purposes, shared with unscrupulous third parties, or retained even when it is no longer relevant at the individual's circumstances have changed.

In order to regulate privacy throughout the use of IoT/IoMT regarding to sensible data, then, perhaps the two main (but not only) legal principles are finality of collected data and non-discrimination. Brazilian legal acts concerning to such matter seem to be attending to such need, but left a huge door open not only to disrespect of privacy by bad intentioned third parties, but also to the government itself, as public policies could make use of sensible personal data in order to attend public interests.

6. REFERENCES

ALLHOFF, Fritz; HENSCHKE, Adam. The Internet of Things: Foundational ethical issues. **Internet of Things**, v. 1–2, p. 55-66, 2018.

ALY, Mohab et al. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. **Internet of Things**, v. 6, p. 1-24, 2019.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, Curitiba, v. 4, n. 3, p. 167-200, set./dez. 2017.

BANNAN, Brenda; GALLAGHER, Shane; LEWIS, Bridget. Next-Generation Learning: Smart Medical Team Training In: GENG, Hwaiyu (Ed.). **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 222-249; p. 222-223.

BOROVSKA, Plamenka. Big Data Analytics and Internet of medical Things Make Precision Medicine a Reality. **International Journal of Internet of Things and Web Services**, v. 3, p. 24-31, 2018.

BOUHAÏ, Nasreddine. The IoT: Intrusive or Indispensable Objects? In BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 10-42.

BULOS, Uadi Lammêgo. **Constituição Federal Anotada.** 11 ed. rev. atual. São Paulo: Saraiva, 2015.

CHAUDHURI, Abhik. **Internet of things, for Things, and by Things**. Boca Raton: CRC Press, Taylor & Francis Group, 2018.

GENG, Hwaiyu. Internet of Things and Data Analytics in the Cloud with Innovation and Sustainability In: GENG, Hwaiyu (Ed.). **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 21-79.

GILBERT, Françoise. Privacy and Security Legal Issues In: GENG, Hwaiyu (Ed.). **Internet of Things and Data Analytics Handbook.** Hoboken: John Wiley & Sons, 2017, p. 1582-1636.

GRAMMATIKIS, Panagiotis I. Radoglou; SARIGIANNIDIS, Panagiotis G.; MOSCHOLIPS, Ioannis D. Securing the Internet of Things: Challenges, threats and solutions. **Internet of Things**, v. 5, p. 41–70, 2019.

GUNTUR, Sitaramanjaneya Reddy; GORREPATI, Rajani Reddy; DIRISALA, Vijaya R. Internet of Medical Things: remote healthcare and Health Monitoring Perspective In: HASSANIEN, Aboul Ella; DEY, Nilanjan; BORRA, Surekha (Ed.). **Medical Big Data and Internet of Medical Things:** advances, challenges and applications. Boca Raton: CRC Press, Taylor & Francis Group, 2019, p. 633-703.

HOLDOWSKY, J. et al. **Inside the Internet of Things (IoT)**. Westlake: Deloitte University Press, 2015.

IEEE Standards Association (IEEE-SA). **Internet of Things (IoT) Ecosystem Study.** IEEE Standards Association, The Institute of Electrical and Electronic Engineers, Inc., 2015. Available at: https://iot.ieee.org/images/files/pdf/iot_ecosystem_exec_summary.pdf. Access in: 4 fev 2019.

MARAS, Marie-Helen. Internet of Things: security and privacy implications. **International Data Privacy Law**, v. 5, n. 2, p. 99-104, 2015.

MATOS, Liliane Gonçalves; MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Limites à implantação de chips subcutâneos: a tutela da privacidade como instrumento de proteção da pessoa na sociedade da informação. **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 18, n. 3, p. 267-300. set./dez. 2017.

MELCHERTS, Helga E. The Internet of Everything and Beyond: the Interplay between Things and Humans In DIXIT, Sudhir (Ed.). **Human bond communication:** the holy grail of holistic communication and immersive experience. Hoboken: John Wiley & Sons, Inc., 2017, p. 439-468.

MIHOVSKA, Albena; PRASAD, Ramjee; PEJANOVIC, Milica. Human-centered IoT Networks In DIXIT, Sudhir (Ed.). **Human bond communication:** the holy grail of holistic communication and immersive experience. Hoboken: John Wiley & Sons, Inc., 2017, p. 178-219.

MILOVANOVIC, Dragorad; BOJKOVIC, Zoran. Cloud-based IoT healthcare applications: Requirements and recommendations. **International Journal of Internet of Things and Web Services**, v. 2, p. 60-65, 2017.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: Uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

NASCIMENTO, Carlos Valder do. Direito fundamental à saúde. In: MARTINS, Ives Gandra da Silva; MENDES, Gilmar Ferreira; NASCIMENTO, Carlos Valdez do (Org.) **Tratado de Direito Constitucional.** 2 ed. São Paulo: Saraiva, 2012, p. 379-437.

NEGASH, Behailu et al. Leveraging fog computing for healthcare IoT In: RAHMANI, Amir M. et al. (Ed.). **Fog computing in the Internet of Things:** intelligence at the edge. Cham: Springer, 2018, p. 336-395.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Coord. Maria Celina Bondin de Morais. Translation to Portuguese by Danilo Doneda e Luciano Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSE, Karen.; ELDRIDGE, Scott D.; CHAPIN, Lyman. The Internet of Things: an overview. **The Internet Society (ISCO)**, 2015.

ROXIN, Ioan; BOUCHERAU, Aymeric. Introduction to the technologies of the Ecosystem of the Internet of Things In: BOUHAÏ, Nasreddine; SALEH, Imad (Ed.). **Internet of Things:** Evolutions and Innovations. Digital Tools and Uses Set series, vol. 4. London: Wiley-ISTE, 2017, p. 104-193.

SÁNCHEZ, Julia et al. Security in Smart Grids In: SUN, Hongjian; WANG, Chao; AHMAD, Bashar I. (Ed.). **From Internet of Things to Smart Cities:** Enabling Technologies. Boca Raton: Taylor & Francis, 2018, p. 433-547.

SFAR, Arbia Riahi et al. A roadmap for security challenges in the Internet of Things. **Digital Communications and Networks**, v. 4, n. 2, p. 118-137, abr. 2018.

SHARMA, Neha; SHAMKUWAR, Madhavi; SINGH, Indjerit. The History, Present and Future with IoT In: BALAS, Valentina et al. (ed.). **Internet of Things and Big Data Analysis for Smart Generation**. Cham: Springer, 2019, p. 101-160.

SINNAPOLU, GiriBabu; ALAWNEH, Shadi. Integrating wearables with cloud-based communication for health monitoring and emergency assistance. **Internet of Things**, v. 1–2, p. 40–54, 2018.

SOLANGI, Zulfiqar Ali et al. **The future of data privacy and security concerns in Internet of Things** In: 2018 IEEE INTERNATIONAL CONFERENCE ON INNOVATIVE RESEARCH AND DEVELOPMENT (ICIRD), 11-12 May 2018, Bangkok. Available at: https://ieeexplore.ieee.org/document/8376320. Access in: Jun 24 2019.

SWAROOP, K. Narendra et al. A health monitoring system for vital signs using IoT. **Internet of Things**, v. 5, p. 116–129, 2019.

TSIATSIS, Vlasos. **Internet of Things:** technologies and applications for a new age of intelligence. 2 ed. London: Academic Press, 2019.

WEBER, Rolf H. Internet of things – Need for a new legal environment? **Computer Law & Security Review**, v. 25, p. 522–527, 2009.

WEBER, Rolf H. Internet of Things – New security and privacy challenges. **Computer Law & Security Review**, v. 26, n. 1, p. 23-30, jan. 2010.

WEBER, Rolf H. Internet of things: Privacy issues revisited. **Computer Law & Security Review**, v. 31, n. 5, p. 618-627, dec. 2015.